Spring 2015

System importance measures: A new approach to resilient systems-of-systems

Payuna Uday
Purdue University

Graduate School Form 30
Updated 1/15/2015

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Payuna Uday

Entitled

System Importance Measures: A New Appraoch to Resilient Systems-of-Systems

For the degree of Doctor of Philosophy

Is approved by the final examining committee:

Karen Marais
Chair

Daniel DeLaurentis

William Crossley

Abhijit Deshmukh

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Karen Marais

Approved by: Tom Shih 04/22/2015

Head of the Departmental Graduate Program Date

SYSTEM IMPORTANCE MEASURES: A NEW APPROACH TO RESILIENT SYSTEMS-OF-SYSTEMS

A Dissertation
Submitted to the Faculty
of
Purdue University
by
Payuna Uday

In Partial Fulfillment of the
Requirements for the Degree
of
Doctor of Philosophy

May 2015
Purdue University
West Lafayette, Indiana

To my parents,

My strength, my inspiration, my reason

ACKNOWLEDGEMENTS

I would like to thank the members of my advisory committee, Dr. Karen Marais, Dr. Daniel DeLaurentis, Dr. William Crossley, and Dr. Abhijit Deshmukh for their advice and insights that have shaped this research. Their invaluable comments and suggestions helped make this dissertation more complete and have greatly contributed to my intellectual growth.

I would especially like to thank my advisor Dr. Karen Marais, for her guidance and continued support throughout my time here at Purdue. I have enjoyed our many wide-ranging discussions and truly believe she is a wonderful mentor for young women in engineering.

The Ph.D. can be a lonely and frustrating experience, but I have had the good fortune of making friends with numerous wonderful people who have made this journey a memorable one.

Having been part of my research group from its inception, I have been blessed with a wonderful succession of colleagues from all over the world over the past six years. We have rejoiced with each other in good times and supported each other through trying ones. I am especially thankful to Nicoletta for everything she has done for me during my last semester: from helping me “drop and jump” to spending an entire day baking goodies for my defense; to Arjun for diffusing many stressful moments with laughter and jokes, and for his valiant efforts in Operation FFP; and last but definitely not least, to Madhur for being my best friend through this journey – you have supported me through one of the

hardest phases in your life and for that, I will always be grateful.

My friends in SERC have been a constant source of happiness over the course of my Ph.D. Zhemei, Cesare, and Navin: I will cherish and truly miss the laughter, teasing, dinners, conversations, and conference escapades. Vi voglio bene!

Many other people have made this experience much more than academic. A special thank you to Jyothi for helping me through some of my darkest days, Senthil for the many fun and light-hearted conversations we've shared, and Dev for being a good friend who is just a call away.

Of course, none of this would have been possible without the constant faith and support of my parents, Uday and Chithra. Your unconditional love and the sacrifices you have made are beyond my ability to describe and cannot be compensated for. This dissertation is yours.

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

Figure Page

ABSTRACT

Uday, Payuna, Ph.D., Purdue University, May 2015. System Importance Measures: A New Approach to Resilient Systems-of-Systems. Major Professor: Karen Marais.

Resilience is the ability to withstand and recover rapidly from disruptions. While this attribute has been the focus of research in several fields, in the case of system-of-systems (SoSs), addressing resilience is particularly interesting and challenging. As infrastructure SoSs, such as power, transportation, and communication networks, grow in complexity and interconnectivity, measuring and improving the resilience of these SoSs is vital in terms of safety and providing uninterrupted services.

The characteristics of systems-of-systems make analysis and design of resilience challenging. However, these features also offer opportunities to make SoSs resilient using unconventional methods. In this research, we present a new approach to the process of resilience design. The core idea behind the proposed design process is a set of system importance measures (SIMs) that identify systems crucial to overall resilience. Using the results from the SIMs, we determine appropriate strategies from a list of design principles to improve SoS resilience. The main contribution of this research is the development of an **aid to design** that provides specific guidance on where and how resources need to be targeted. Based on the needs of an SoS, decision-makers can iterate through the design process to identify a set of practical and effective design improvements.

We use two case studies to demonstrate how the SIM-based design process can inform decision-making in the context of SoS resilience. The first case study focuses on a naval

warfare SoS and describes how the resilience framework can leverage existing simulation models to support end-to-end design. We proceed through stages of the design approach using an agent-based model (ABM) that enables us to demonstrate how simulation tools and analytical models help determine the necessary inputs for the design process and, subsequently, inform decision-making regarding SoS resilience.

The second case study considers the urban transportation network in Boston. This case study focuses on interpreting the results of the resilience framework and on describing how they can be used to guide design choices in large infrastructure networks. We use different resilience maps to highlight the range of design-related information that can be obtained from the framework.

Specific advantages of the SIM-based resilience design include: (1) **incorporates SoS-specific features within existing risk-based design processes** - the SIMs determine the relative importance of different systems based on their impacts on SoS-level performance, and suggestions for resilience improvement draw from design options that leverage SoS-specific characteristics, such as the ability to adapt quickly (such as add new systems or re-task existing ones) and to provide partial recovery of performance in the aftermath of a disruption; (2) **allows rapid understanding of different areas of concern within the SoS -** the visual nature of the resilience map (a key outcome of the SIM analysis) provides a useful way to summarize the current resilience of the SoS as well as point to key systems of concern; and (3) provides a platform for multiple analysts and decision-makers to **study, modify, discuss and document** options for SoS.

CHAPTER 1. INTRODUCTION

1.1 Background and Motivation

All systems are subject to change during their operational lifetime. Resilience is the ability of a system, process or organization to react to, survive, and recover from adverse changes (disruptions). By virtue of its importance, this attribute drives important design and development decisions in systems engineering and management. The characteristics and features that make a system resilient can also significantly affect the cost and schedule of large development projects since resilience implementation consumes resources and may therefore require tradeoffs in system functionality. Thus, due to the often expensive nature of resilience, maintaining or improving performance is frequently given priority, resulting in systems that are (partly) resilient to only a small set of disruptions. Additionally, long-lasting systems, such as infrastructure networks (e.g., energy, transportation, communications), may be resilient to certain disruptions, but as time passes after the system is fielded, changes in the operating environment may make the networks less resilient to both old and new types of threats.

Systems-of-systems (SoSs) is a term that has gained traction over the past several years to describe networks of independently operating heterogeneous systems that interact with one another to provide an overall capability, which cannot be achieved by the individual systems alone [White, 2006]. Examples of SoSs include the United States Air Transportation System (ATS) and tactical SoSs used by the military. Figure 1.1 illustrates a littoral combat SoS. The mission comprises aircraft carriers, littoral combat ships (LCS), unmanned surface vehicles (USV), unmanned aerial vehicles (UAV), and helicopters. These systems work together to detect and neutralize enemy agents, such as ships,

submarines, and mines. Each system performs one or more functions; collaborations between systems enable higher-level mission capabilities.

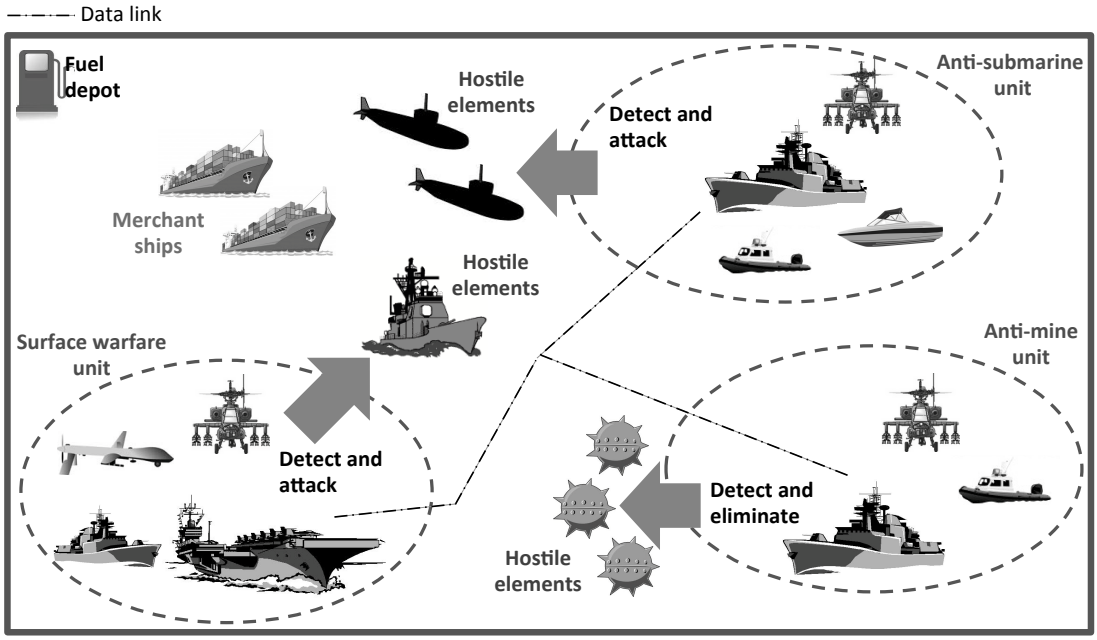

Figure 1.1 Illustrative Littoral Combat SoS

Given the importance of systems-of-systems, managing SoS resilience is vital to national security, global economies, and in many cases, public health and safety. There are many reasons why an SoS may not be resilient: design flaws, unanticipated disruptive events, emergent behavior of operational evolution (such as technological and software upgrades), poor contingency planning and execution, and limitations at the organizational level. Thus, while the resilience of SoSs depends in part on the reliability of their constituent systems, traditional reliability and risk approaches do not provide adequate guidance on how to achieve or manage resilience. Given the diversity and often wide geographic distribution of SoS constituent systems, inclusion of backup systems for a SoS is usually impractical and costly. Additionally, high levels of interdependency between the systems imply increased risks of failures cascading throughout the SoS. At the same time, the features (such as heterogeneity) giving rise to these hurdles also offer

the opportunity to improve the resilience of the overarching system through unconventional means.

To illustrate the above observations, consider, for example, a critical infrastructure SoS, such as the national transportation network. At present, research, development, and operation for each sector of the United States National Transportation System (NTS) is generally conducted independently, with little consideration of multi-modal impacts, societal and cultural influences, and network interactions [DeLaurentis et al., 2007]. Typically, resilience is addressed at a modal level: the robustness of a particular transportation network is addressed independently of other modes of transportation. Designers assume that the remaining transportation network is available when one part of one mode fails. For example, when a subway line is suddenly unavailable due to some failure or threat, the unmet demand spills onto the road network (comprising buses and automobiles). Individual organizations that cover several modes, such as for example the Massachusetts Bay Transportation Authority (MBTA), do plan for such disruptions to some degree, but there is less coordination between organizations. Thus, for example if Logan Airport closes due to weather, AMTRAK rail service cannot meet all the spillover demand in a reasonable time. There may also be interdependencies between modes. For example, in the aftermath of Hurricane Sandy in 2012, while the airports in New York were able to resume operations relatively quickly, road and rail services took longer to provide adequate services. As a result, airline employees were unable to get to work at the airports and airlines had to fly in technology specialists and customer service agents from Atlanta to maintain their specific airport operations [Brown and Drew, 2012]. In contrast, in the weeks after an earthquake in southern California (1994), although Los Angeles road networks were critically impacted, rail services resumed relatively quickly. In particular, the existence of a separate freight rail system in the city allowed officials to augment the commuter rail services by using the cargo line during this period [Giuliano and Golob, 1998].

As systems continue to grow in scale and complexity, several research efforts have focused on developing methods for engineering resilient systems. For example, Engineered Resilient Systems was identified as a strategic investment priority by the United States Department of Defense as part of its program objectives for 2013-2017 [DoD, 2011]. Also, the International Council on Systems Engineering (INCOSE) has a dedicated working group for Resilient Systems that shapes research on the use of systems engineering practices to achieve resilience [INCOSE, 2000]. The Resilience Alliance [2001] is another research organization that facilitates research in the scientific community with the specific aim of improving resilience in socio-ecological systems. The interest in resilience has led to significant developments in studies and models, but our review of the literature reveals that the research on SoS resilience is still in its nascent stages in terms of defining, measuring, and identifying methodologies to achieve resilience.

Resilience management is a process that allows decision-makers to systematically evaluate, improve, and maintain resilience. Contrary to risk management which asks "*what could make the lights go out?*" resilience management shifts focus to "*it does not matter what makes the lights go out, how are we going to deal with it if they do?*" [Dalziell and McManus, 2004]. Specific questions that need to be answered to manage resilience in SoSs can be grouped into three key focus areas (see Figure 1.2):

1. What is resilience in the context of an SoS and when is it appropriate?
    - How can resilience be distinguished from other system-level attributes?
2. How can resilience be designed?
    - What level of resilience is desirable and how resilient is the SoS currently?
    - What principles can be applied to achieve resilience in SoS design?
3. How can resilience be maintained over the SoS lifetime?
    - When does resilience change?
    - How can adverse impacts of changing resilience be observed and mitigated?

The answers to these questions lie in a wide range of fields, reflecting the diverse and complex nature of SoSs. While a comprehensive treatment of the topic should address the three questions, it would be ambitious and impossible to address all three questions adequately in a single thesis. Instead, here, we **focus on the first two questions and present a new approach to aid the design of resilient SoSs**. We now provide a brief overview of systems-of-systems and conclude the chapter with specific contributions of this thesis.

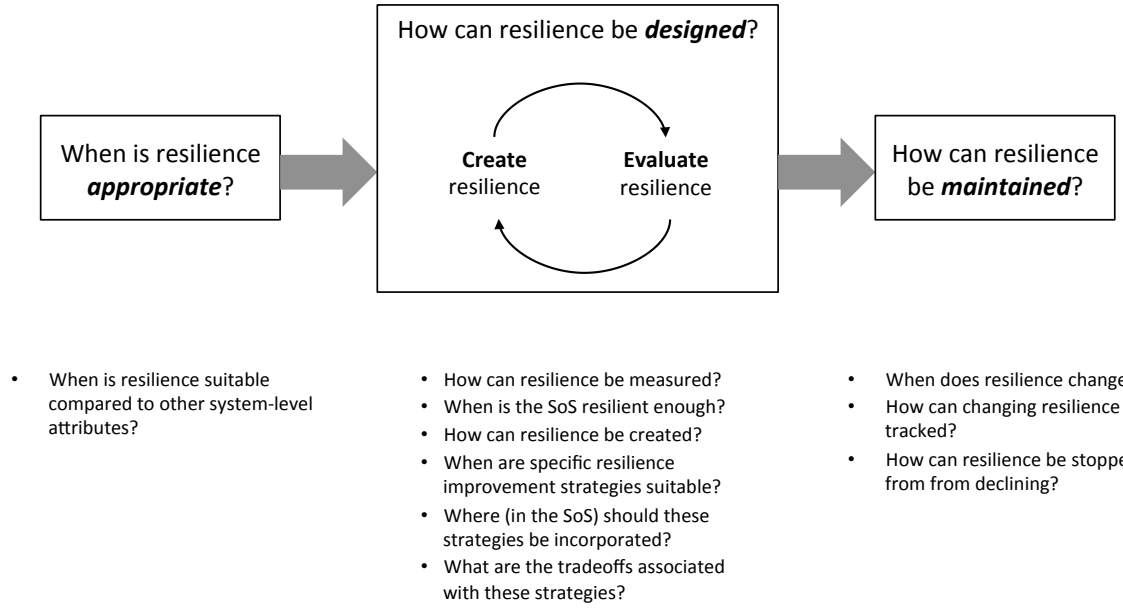

Figure 1.2 Key aspects of resilience management

1.2 Systems-of-Systems: A Brief Overview

In this section, we provide a brief overview of systems-of-systems (SoSs). The interested reader is referred to Crossley [2004], Abbot [2006], Dahmann and Baldwin [2008], DoD [2008], Jamshidi [2008], Gorod and Sauser [2008], Luzeaux [2011], Barot et al. [2013], and TTCP [2014] for a broader discussion of SoSs.

The emergence of complex systems over the past few decades has led to increased interest in exploring methods to incorporate inherent resilience within them. A complex system can be defined as " an open system with continually cooperating and competing elements – a system that continually evolves and changes according to its own condition and external environment" (White, 2006). Examples of complex systems include satellites, aircraft, and submarines. These systems are expensive to design and build, they operate in harsh or remote environments, and any failure of these systems is typically a high publicity event. In some cases, such as satellites, maintenance and repair is difficult or impossible in physically inaccessible environments.

In recent years, networks of complex systems, known as system-of-systems (SoS), have garnered increased attention [DeLaurentis et al, 2011; McCarter and White, 2007]. Formally, the term system-of-systems is used to denote networks that are formed from the integration of independently operating complex systems that interact with one another to provide an overall capability, which cannot be achieved by the individual systems alone [White, 2006]. Examples of SoSs include the national air space (NAS) and the United States military's ballistic missile defense system. These meta-systems are characterized by the operational and managerial independence of the constituent systems, the evolutionary nature and emergent behavior of the larger SoS, and the geographic distribution of the sub-systems [Maier, 1998]. High levels of interdependency add to the overall complexity of the SoS.

These large-scale meta-systems exist within a spectrum that contains ad-hoc, short-lived SoSs on one end, and long-lasting, continually evolving SoSs on the other end [Jamshidi, 2008]. Two examples within the engineering domain further illustrate this idea. Military operations where combinations of various air, ground, and naval units collaborate to perform a particular mission fall into the former portion of this continuum. On the other hand, large-scale transportation networks, such as the NAS or even the national highway system (NHS), have been established to provide services for many decades, and are always in a state of continual improvement, and in several cases, deterioration.

The primary driver behind the SoS perspective was the need to obtain higher-level capabilities and performance than would be possible with a traditional systems view. The SoS outlook presents a high-level viewpoint and explains the interactions between each of the independent systems. Hence, while SoS engineering has its roots in the established systems engineering discipline, addressing the needs and design of SoSs goes beyond traditional systems engineering in a number of ways, as shown in Table 1.1.

Table 1.1 Differences between traditional systems engineering (SE) and system-of-systems engineering (SoSE) (Adapted from Duffy et al. [2008])

	SE perspective	SoSE perspective
Scope	• Project/product • Autonomous/we-bounded	• Enterprise/capability • Interdependent
Objective	• Enable fulfillment of requirements • Structured project process	• Enable evolving capability • Guide integrated portfolio
Time frame	• System lifecycle • Discrete beginning and end	• Multiple, interacting system lifecycles • Amorphous beginning
Organization	• Unified and authoritative	• Collaborative network
Development	• Design follows requirements	• Design is likely legacy-constrained
Verification	• System in network context • One time, final event	• Ensemble as a whole • Continuous, iterative

Interest in analyzing, designing, and improving attributes such as performance and robustness of SoS has spurred research in these characteristics. For example, SoS-related challenges are the focus of research in various domains such as manufacturing, aerospace, military, service industries, and environmental systems [Crossley 2004; Lopez 2006; Wojcik and Hoffman, 2006]. Some of these challenges include acquiring systems for the SoS, managing the interfaces between the heterogeneous systems, understanding adaptive and emergent behavior of the composite systems, accounting for a diversity in the management and stakeholders associated with different parts of the SoS, and considering the staggered inclusion and exclusion of systems in the overarching system over time. In this thesis we focus on the resilience of SoSs and present an approach to designing

resilient SoSs. Next, we highlight some of the challenges and opportunities for resilience design in SoSs.

Typically, the systems in an SoS are individually acquired and integrated into the larger structure. Also, the design and development of these systems are generally independent of each other. For instance, although almost every military system is operated as part of a system-of-systems, most of these systems are optimized sequentially (i.e., the new system must fit well in the existing context) [Jamshidi, 2008], rather than holistically (i.e., how should new, existing, and possible future systems be combined to maximize desired SoS attributes (e.g., Mane et al. [2007]). In unfortunate cases, this insular systems development practice can lead to failures and undesired emergent behavior of the overall SoS, as shown in the earlier Hurricane Sandy example.

Interfaces are critical areas of concern for SoS development. Apart from impacting the seamless integration of different systems, a direct consequence of interfaces is the creation of interdependencies between the constituent systems. Further, as SoSs themselves evolve into even more complex networks, the links between SoSs (e.g., between communications and energy networks) are gaining increased attention [Thissen and Herder, 2008; Zio and Ferrario, 2013].

From an organizational standpoint, the wide range of owners, managers, and stakeholders of the systems constituting the SoS increases uncertainty and complexity. For example, the global air transportation system (ATS) architecture is driven by the goals of regional and global economies. It comprises multiple stakeholders such as regulatory authorities, aircraft manufacturers, air traffic control, airlines, airports, and the flying public. Each one is concerned with maximizing its own objectives. Air traffic control is concerned with flight safety and maximizing throughput, the airlines are concerned with maximizing profits, airports are concerned with conserving costs while providing acceptable service, and the passengers are interested in getting the best value (low fares, minimum delay, and good customer service) from the ATS.

Finally, SoSs are typically never fully formed or complete [Abbot, 2006]. Their development is evolutionary and adaptive as components, functions, and goals, are added, removed, and modified over time. For example, while NextGen aims at transforming (through upgrades and new technology) the United States airspace to achieve better operational and environmental efficiency, several critical legacy systems will still be part of the overall system. This implies that key SoS characteristics, such as performance and resilience, must be constantly reviewed as the systems and their operating environments change with time.

Based on the type of central control and organizational hierarchy of the constituent systems, SoSs can be classified as directed, virtual, collaborative, or acknowledged [Maier, 1998; Dahmann and Baldwin, 2008; DeLaurentis et al, 2011]. Directed SoSs (e.g., Integrated Air Defense) are centrally managed to fulfill specific purposes. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose. On the other hand, virtual SoSs (e.g., the World Wide Web) lack a central management authority and a centrally agreed-upon purpose for the system-of-systems. Large-scale behavior emerges, and may be desirable, but this type of SoS must rely on relatively invisible mechanisms to maintain it. In collaborative SoSs (e.g., the Internet), the component systems interact more or less voluntarily to fulfill agreed upon central purposes. Finally, acknowledged SoSs (e.g., Ballistic Missile Defense System) have recognized objectives, a designated manager, and resources. However, the constituent systems retain their independent ownership, objectives, funding, development, and sustainment approaches. This difference in central control architecture impacts the interfaces between the constituent systems as well as the interactions experienced at the system boundaries, resulting in implications for the design and optimization of key attributes such as resilience [Barot et al., 2013].

1.3 Terminology

This section defines various terms that will be referred to in this thesis.

Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions [PPD, 2013].

Resilience management. The process of evaluating, improving, and ultimately maintaining resilience at an acceptable level throughout the lifetime of an SoS.

Disruption. An event that can interrupt some activity or process (of the SoS).

Restoration. A strategy to return to nominal SoS performance level after a disruption (through the repair or replacement of the disrupted entities).

Mitigation/Recovery. A strategy to reduce the impact of a disruption.

1.4 Thesis Outline and Contributions

In this thesis, we focus on the first two questions that drive resilience management (see Section 1.1) and present a new approach to guide the design of resilient SoSs:

1. What is resilience in the context of an SoS and when is it appropriate?
    - How can resilience be distinguished from other system-level attributes?
2. How can resilience be designed?
    - What level of resilience is desirable and how resilient is the SoS currently?
    - What principles can be applied to achieve resilience in SoS design?

Chapter 1 has introduced the concept of resilience and its importance with respect to systems-of-systems.

The purpose of Chapter 2 is to answer the first question: when is resilience appropriate (compared to other system attributes) in the context of SoSs? The research follows a

review of the concept of resilience as discussed in various fields of investigations, and a comparison with related engineering attributes such as reliability, robustness, and flexibility. It is seen that characterizing the purpose of the different attributes is useful in enriching SoS design in specific ways.

Chapters 3 and 4 focus on the second question in resilience management: how can SoS resilience be designed? In Chapter 3 we review and integrate the progress on addressing this question. Methods, tools, and processes that can be applied to designing resilient SoSs are categorized and discussed. We observe that traditional risk and reliability tools have use in assessing resilience but that their application has limitations. Instead recent multi-disciplinary research that has made significant strides in modeling and evaluating SoSs can be leveraged more effectively to address this issue. Based on this review, we conclude that a key gap in addressing SoS resilience is in providing informative design guidance. Additionally, a major outcome of this chapter is the synthesis of a set of design principles that be applied to the design of resilient SoSs.

Chapter 4 presents a new approach to resilience design. The core idea behind the proposed design process is a set of system importance measures (SIMs) that identify systems crucial to overall resilience. Using the results from the SIM analysis, we determine appropriate strategies from a list of design principles to improve SoS resilience. The main contribution of this research is the development of an **aid to design** that provides specific guidance on where and how resources need to be targeted. Based on the specific needs of an SoS, decision-makers can iterate through the design process to identify a set of practical and effective design improvements.

Chapter 5 demonstrates the applicability of the SIM-aided design approach through two case studies: a naval warfare SoS and an urban transportation SoS. Each case study draws attention to different aspects of the resilience design. In the naval warfare case study, we illustrate how the design process can leverage existing simulation tools and analytical models to support end-to-end design. The urban transportation case study instead focuses

on interpreting the results of the design process and on describing how they can be used to guide design choices in large infrastructure networks.

Chapter 6 summarizes the contributions of this research and provides suggestions for future work. This chapter also highlights key challenges in designing SoS resilience and presents a series of research needs that can provide direction to research endeavors in this field.

CHAPTER 2. DEFINING RESILIENCE IN THE CONTEXT OF AN SoS

The purpose of this chapter is to understand and clearly define *resilience* in the context of a system-of-systems. First, we review the concept of resilience as discussed in various fields. Next, we make the case of resilience in SoSs by contrasting it with related engineering attributes, such as robustness, survivability, reliability, flexibility, pliability, agility, and safety.

2.1 A Multi-Disciplinary Review of Resilience

There is a growing body of research on resilience in a diverse set of fields, such as ecology, economics, organizational science, and engineering. While the specific definition of resilience varies between domains, intrinsic to the notion of resilience is the ability to respond to and quickly recover from catastrophic events. This section briefly discusses how resilience is viewed in various fields. The interested reader is referred to Francis and Bekera [2014] for a comprehensive review of resilience definitions in different disciplines.

While the concept of resilience has been applied in a variety of diverse domains, there is little consensus on the origins of the concept: some scholars claim that the construct of resilience began in physics [Van der Leeuw and Leygonie, 2000], others contend that its popularity stemmed from its discussion in child psychology [Kantur and Iseri-Say, 2012], and yet others claim that Holling's [1973] seminal work in ecology led to the term gaining currency. In physics, resilience describes the physical property of a material that characterizes its resistance to shocks [Manyena, 2006]. Research in psychology and ecology adopted a similar interpretation of resilience; here, the term emphasizes the capacity to resist disruptions or to return to equilibrium after perturbations. For example,

in psychology, studies on the children of schizophrenic parents [Garmezy, 1970] and on children in the island of Kauai–Hawaii [Werner and Smith, 1977], suggest that resilience, as a personality trait, was the key contributing factor behind the survival of adversely affected children. These ideas were extended to the larger society in that individuals and families are said to "demonstrate resilience when they draw on inner strengths, skills, and supports to keep adversity from derailing their lives" [Johnson and Wiechelt, 2004]. In general, most researchers agree that psychological resilience refers to successful adaptation despite risk and adversity [Masten, 1994], or unexpected achievement in spite of stress [Bartelt, 1994].

In the ecology literature, the term resilience has grown to describe two views [Holling, 1996]. The first definition focuses on the ability of a system to maintain a fixed equilibrium point. Here, resistance to a disturbance and the rate of return to the equilibrium point are used to measure the resilience of the system. In contrast, the second definition moves away from this traditional homeostatic approach and concentrates on the ability of a system to move into a different equilibrium or stable state to maintain functionality in the face of a disruption [Holling, 1973]. While the first perspective has provided the foundations for the development of economic and engineering resilience, the second view is largely observed in the ecological sciences. We believe that this second definition of resilience will have greater implications in the engineering domain as systems grow in complexity and scale (this idea is discussed further in Section 6.2.2).

The concept of resilience has also been widely discussed in the disaster management literature. Wildavsky [1991] defines resilience as "the capacity to cope with unanticipated dangers after they have become manifest". This definition concentrates on those events that cannot be anticipated and on the post-event state, whereas resilience is also relevant when there is a certain level of anticipation and preparedness at the pre-event state. Thus, the term refers to the capacity to adjust to foreseen disruptions as well as to adapt to unpredictable, sudden, shocks [Tierney, 2003].

In organizational studies, resilience has been defined as the ability of an organization to "keep, or recover quickly to, a stable state, allowing it to continue operations during and after a major mishap or in the presence of continuous significant stresses" [Wreathall, 2006]. Hamel and Valikangas [2003] state that revolution, renewal and resilience are three important states of turbulent times and that resilience is related to the constant reconstruction of organizational values, processes and behavior. It is interesting to note that, in addition to disasters that are one-time disturbances with severe consequences, daily operations of rapidly changing business environments also require resilience for survival. Mallak [1998] states that resilience is not just required under sudden shocks such as natural disasters or terrorist attacks, but also relevant for employees faced with continuous transformation of business environments. Some scholars [Sheffi, 2007; Weick et al., 1999] also argue that resilient investments can be turned into competitive advantage. As Folke [2006] states, "disturbance has the potential to create opportunity for doing new things, for innovation, and for development". In line with the same reasoning, Lengnick-Hall and Beck [2003] define resilience as more than bouncing back—it is also about turning challenges into opportunities and thereby creating superior performance than before. This proactive notion of resilience challenges the single-equilibrium orthodoxy and further highlights the potential of systems to transition to new, less vulnerable steady states.

In the engineering domain, resilience is still a relatively new concept, and several definitions have been put forward to define this system characteristic. In Hollnagel et al. [2006], an early collection of work on resilience in the engineering domain, resilience is defined as the "ability of a system or organization to react to and recover from disturbances at an early stage with minimal effect on its dynamic stability". Another closely related definition, given by INCOSE's Resilient Systems Working Group, states that resilience is the "capability of a system with specific characteristics before, during and after a disruption to absorb the disruption, recover to an acceptable level of performance, and sustain that level for an acceptable period of time" [INCOSE, 2000]. Resilience engineering has its roots in the well-established fields of reliability and safety

management. The idea of a resilient system builds upon foundational concepts in both these fields and applies them to modern-day complex systems. Today, resilience has taken on a broader scope than previous definitions: in engineered systems it involves a wide range of potential threats and system responses, both preemptive and post event [Jackson and Ferris, 2013].

In recent years, resilience in the cyber domain has received growing attention. As stated by Goodyear et al. [2010], "threats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies". Large-scale socio-technical systems, such as electrical grids and even manufacturing supply chains, are increasingly supported by complex software. While this reliance on cyber infrastructure reflects the need to improve efficiencies and lower costs, risks from cyber intrusions and targeted cyber attacks have important implications for critical civilian and military infrastructures [Chittister and Haimes, 2011]. These concerns have prompted research efforts on resilience in several fields, such as, smart-grid operations [Pearson, 2011], wireless data networks [Yue, 2003], and military operations [Goldman et al., 2011].

In summary, if resilience is to inform design and policy decisions, there is a need to address fundamental questions that continue to blur the concept. Specifically, to enhance resilience in any field it is necessary to have a good understanding of what resilience is, what its determinants are [Klein et al., 1998], and how it can be measured, maintained and improved [Klein et al., 2003].

2.2 Resilience and Related System-Level Attributes

Resilience is one member of an expanding family of system-level attributes. This section reviews the attributes that are closely related to resilience such as survivability, reliability, robustness, and safety. We present the fundamental idea behind each system attribute and compare it with resilience. We also provide illustrative examples to show that making

these distinctions has value in that it adds to the richness of overall SoS design and development.

There are many different ways to distinguish between these system-level attributes, or "ilities". For example, Chalupnik et al. [2013] define these attributes based on the design changes required (or not) for a product or process to respond to off-nominal conditions. Here, we take a system requirements perspective and apply it to different levels in the SoS. This approach allows us to focus on the implications of each attribute for engineering decision-making. All the characteristics discussed here deal with the idea of a system having to cope with or adjust to some kind of change, after it has been fielded. This change can be either: *external*, for instance, disruptions due to operating environment threats, changing policies, and global economics, or *internal*, for instance, component and link failures. In some cases, the differences between the definitions are explicit, while in others the differences are subtler. We classify the attributes on the basis of the impact the change has on the system requirements, as shown in Figure 2.1. In some situations, systems are expected to meet their original requirements in the face of a disruption. Qualities that attempt to satisfy these *constant* system requirements during the disturbance include resilience, robustness, reliability, and survivability. In other cases, the system goals and requirements themselves vary in order to maintain functionality during and after perturbations. Attributes that allow a system to satisfy new or variable requirements include flexibility, agility, and pliability. We do not consider these attributes further here, the interested reader is referred to Saleh et al. [2009] and Ryan et al. [2013] for reviews of flexibility; Mekdeci et al. [2012] discuss pliability; and Dove [2001] and Albert and Hayes [2003] discuss agility.

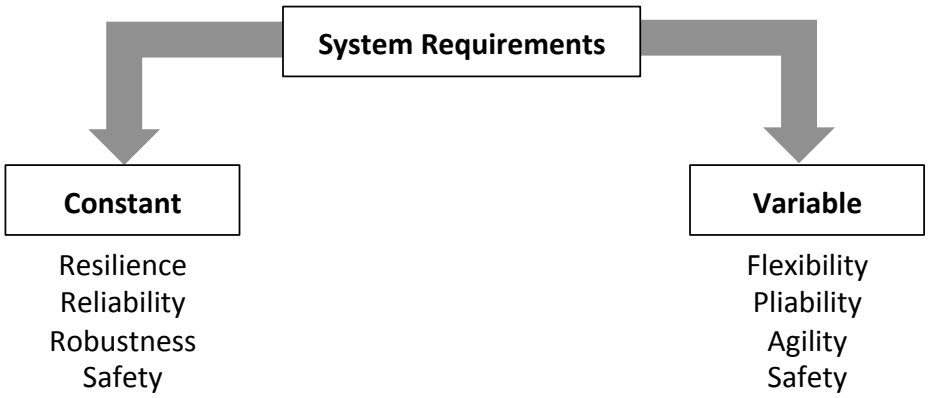

Figure 2.1 Classification of attributes based on system requirements

2.2.1 Defining Resilience

In the engineering domain, several definitions have been put forward to describe resilience. For instance, in Hollnagel et al. [2006], an early collection of work on resilience, resilience is defined as the "ability of a system or organization to react to and recover from disturbances at an early stage with minimal effect on its dynamic stability". More recently, the Presidential Policy Directive (PPD-21) on Critical Infrastructure Security and Resilience states "*resilience* means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [PPD, 2013]. See also [INCOSE, 2000], Laprie [2008], Jackson [2010], and Ruault et al. [2012] for similar definitions.

Resilience is usually represented as a combination of survivability and recoverability, as shown in Figure 2.2[1]. This notional representation is widely used in the literature to

[11] Several definitions for resilience have been proposed in the literature. Some authors view resilience as a superset of two attributes: surviving the disruption and then recovering from it. Others consider survivability to be the overarching attribute. For example, according to Richards et al. [2009], survivability (a property that has emerged from the development of military systems and describes the ability of systems to minimize the impact of finite-duration disturbances on value delivery) consists of three aspects: Type I survivability deals with reducing the likelihood or magnitude of a disturbance; Type II minimizes performance (value) loss in the immediate aftermath of a disturbance; and finally Type III survivability enables the recovery of value delivery in a defined period of time.

depict the fundamental ideas behind resilience (e.g., Tierney and Bruneau [2007], Castet and Saleh [2012], and Ayyub [2014]). Resilience, in other words, is not only concerned with reducing the likelihood of failure. It also stresses the need to recover from unexpected disturbances in the operating environment. Essentially, resilience implies the ability of a system to "bounce back" [Madni and Jackson, 2009] and hence, is a function of several system properties, including component reliability, re-configurability of the architecture, and diversity of sub-systems and components. Resilience can be divided into two categories [Rose, 2007; Whitson and Ramirez-Marquez, 2009]: (1) "static resilience" is related to the "ability of an entity or a system to maintain function", or to survive, when disrupted; while (2) "dynamic resilience" deals with recovery of the system after a shock. We agree with this perspective wherein resilience is characterized as a combination of survivability and recoverability, with an emphasis on the ability of systems to rebound after a disruption.

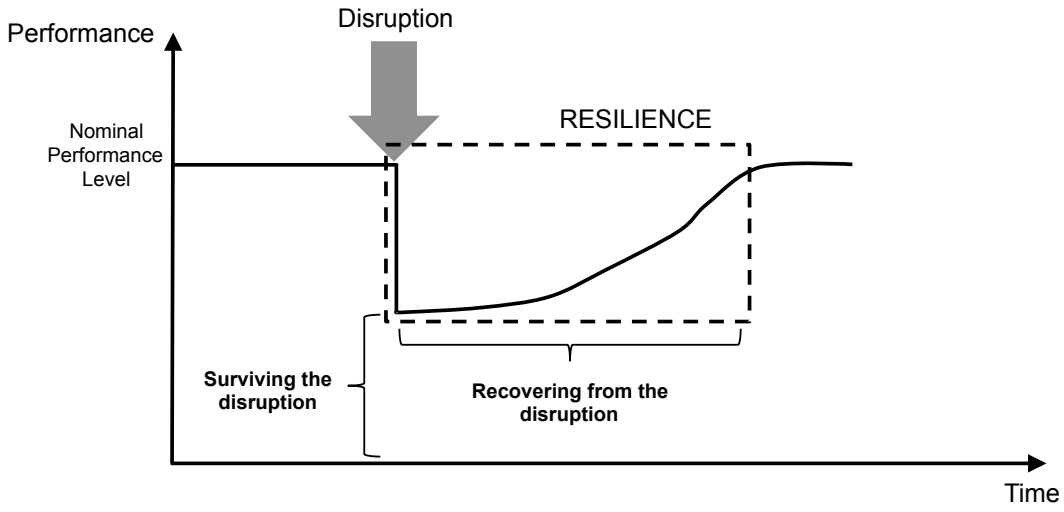

Figure 2.2 Notional depiction of resilience following a disruption ("resilience curve")

An important aspect of resilience definition and characterization is performance. For most SoSs, performance is a complex metric requiring consideration of multiple capabilities. For example, overall performance of the air transportation SoS is some function of, among others, flight schedules, delays, fares, and customer service. This is

primarily due to the diversity in stakeholders and the objectives that are important to them. The objectives for each stakeholder within the air transportation system, and therefore the performance metrics applicable to each, can vary widely: air traffic control is concerned with flight safety and maximizing throughput; the airlines are concerned with maximizing profits; airports are concerned with conserving costs; while providing acceptable service, and the passengers are interested in getting the best value (low fares, minimum delay, and good customer service) from the ATS. Specifically, in any resilience analysis, the choice of the performance metric needs to be documented well so that it is clear to the decision-makers what SoS objectives are being considered (or not considered) for resilience-related decisions. Table 2.1 lists some example SoS performance metrics for various systems-of-systems.

Table 2.1 Example SoS performance metrics

System-of-Systems	Performance metrics
National Air Space	Average delay, throughput, passenger capacity
Space SoS	Carrier/Noise Ratio
Urban Transportation	Average delay, throughput, passenger capacity
Urban water supply	Water production capacity, water available for consumption
Military Reconnaissance Mission	Area imaged, number of targets identified
Military Combat Mission	Mission success

Resilience is highly context dependent – it depends on the structure (architecture) of the system (which could be an SoS, an organization, a network, etc.), its operational environment, and the disruptive event. For example:

- Different systems are resilient to different disruptions. For instance, Chicago O'Hare International Airport (ORD) is reasonably well equipped to handle snowstorms, but 3 inches of snow in southern US caused Atlanta Hartsfield-Jackson International Airport (ATL) to shut down in early 2014 [CBS, 2014].

- A system could be resilient to one type of disruption but not to another type. For example, an airport can be resilient to thunderstorms but may be vulnerable to cyber-attacks on its security systems.

Figure 2.3 and Figure 2.4 highlight a couple of extreme cases of variation in the resilience curve. Sometimes, in the aftermath of a disruption, the performance drop does not necessarily happen steeply and suddenly. During the time between a disruptive event and the full impact, performance usually starts to deteriorate and a more *gradual decline* may be observed [Sheffi and Rice, 2005]. For example, when access to critical automotive components was blocked during the 2002 West Coast port lockout, instead of halting production immediately, logistical constraints meant that it took New United Motor Manufacturing Inc. (NUMMI) four days to stop all assembly activities [Sheffi and Rice, 2005]. Similarly, there are several different ways an SoS can recover from disruptions. Recovery measures can include an *increase in performance* for some time after a recovery to make up for lost capability (see Figure 2.3). For instance, NUMMI used airfreight to get parts to the plants during the port lockout and then made up for closures by running at higher-than-normal utilization to make up for lost production. Conversely, in other cases, despite adequate recovery, disruptions can have *long-term impacts* on SoSs (see Figure 2.4). For example, the network of small-scale shoe factories in Kobe, Japan, lost 90% of its business in the wake of the 1995 earthquake as buyers shifted to other Asian factories, and most buyers never came back [Sheffi and Rice, 2005]. Another example of long-term impact is the increased costs of computer hard drives through 2013, after the 2011 floods in Thailand (second largest computer hard drive supplier in the world) [WEC, 2013].

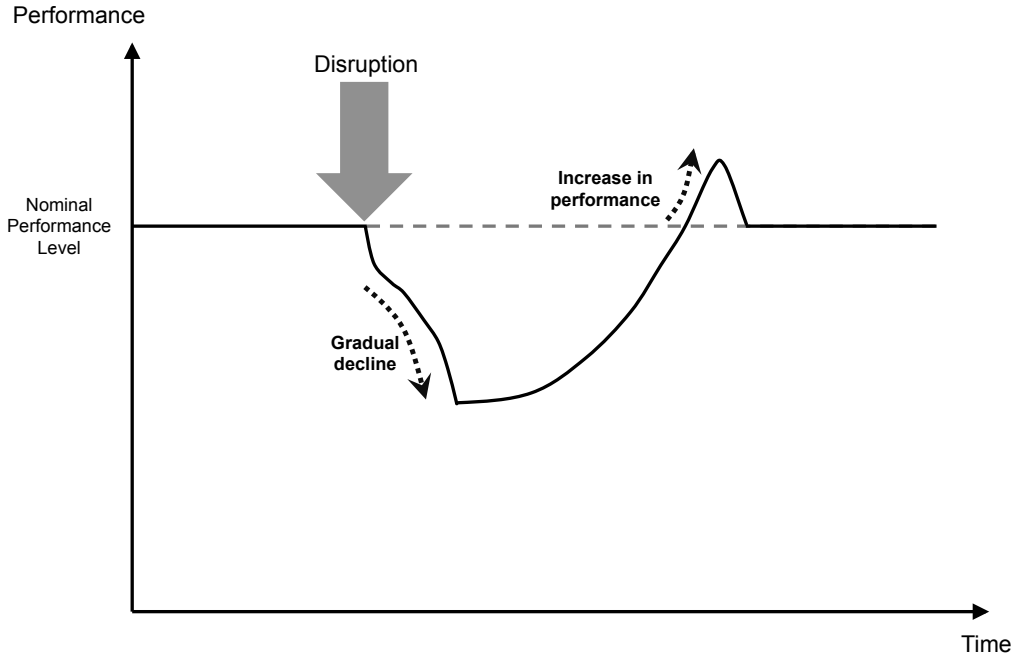

Figure 2.3 Recovery measures can result in a temporary increase in performance

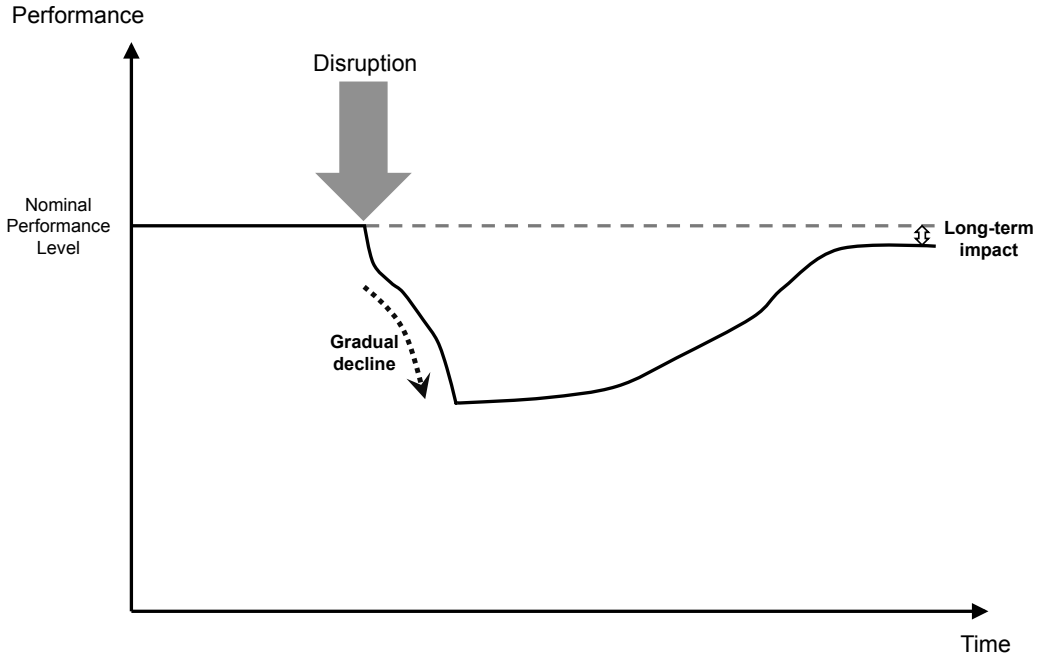

Figure 2.4 Disruptions can result in long-term impacts on performance

Returning to resilience characterization, one way to represent resilience qualitatively is shown in Figure 2.5. A highly resilient SoS is one that experiences a small drop in performance (high survivability) and recoups quickly (high recoverability) after a disruptive event, as shown in the top right hand corner. Conversely, an SoS with low resilience is one that incurs a large performance drop (low survivability) and takes a long time to recover (low recoverability), as indicated in the bottom left hand corner of the figure. For example, as mentioned previously, the National Airspace System is highly resilient to a moderate snowstorm in Chicago (the airports in the region are well-equipped to maintain functionality as long as possible and to resume services quickly once the storm passes) but exhibits low resilience to an equally powerful snowstorm in Atlanta (currently airports in this region are less prepared to handle snowstorms with respect to having adequate runway clearing facilities and de-icing facilities). Finally, moderate resilience can be observed in two ways: high survivability-low recoverability or low-survivability-high recoverability (e.g.: New York city airports had to shut down during Hurricane Sandy but were able to recover relatively quickly compared to the road and rail services in the city).

Next, we contrast the related system-level attributes with resilience, and discuss when each attribute is appropriate.

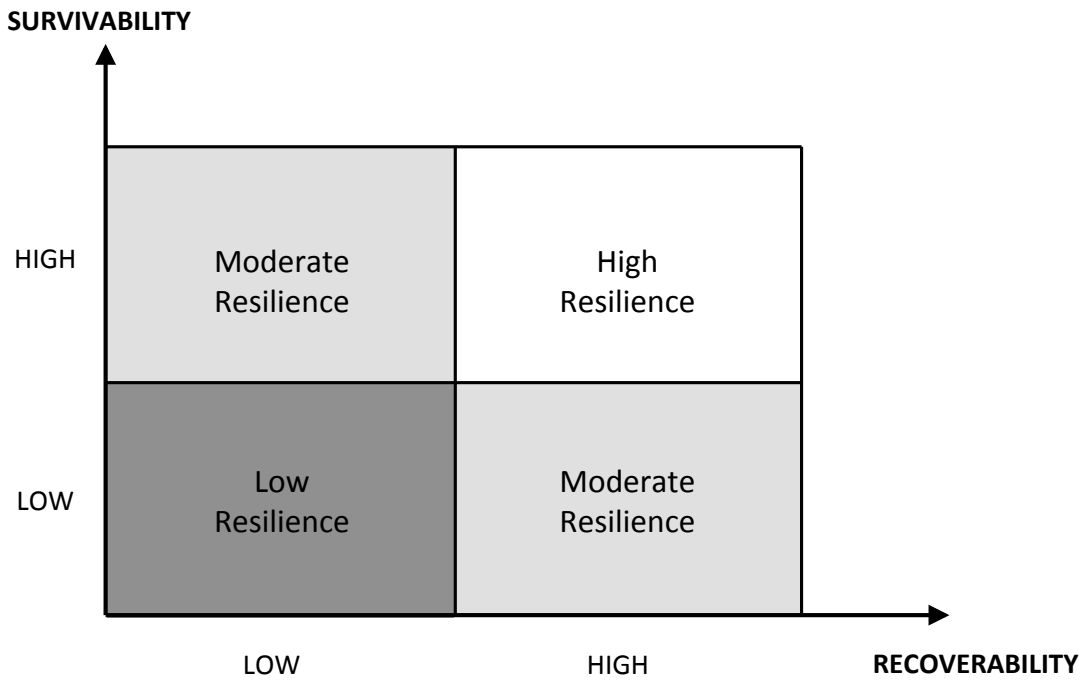

Figure 2.5. Levels of resilience

2.2.2 Reliability

Formally, *reliability* in the engineering domain is the ability of a system and its components to perform required functions under stated conditions for a specified period of time (e.g., Modarres et al. [1999], Rausand and Høyland [2004], and Madni and Jackson [2009]). Reliability is now a mature topic in the literature and a variety of methods exist that enable the design of reliable components and systems. However, as systems become more complex and interdependent, understanding reliability in the context of the resulting SoSs is not necessarily straightforward or trivial. To illustrate the nuances of reliability and resilience implications from an SoS perspective we compare these attributes at different levels of the air transportation system, as shown in Table 2.2. The SoS builds upwards from lower-level components (e.g., fuel selector valves on aircraft), to systems (e.g., aircraft), and finally to the highest-level SoS (the ATS).

Table 2.2 Reliability and resilience considerations at different levels of SoS hierarchy

SoS element	Example	Comparison between reliability and resilience implications
Component	Fuel selector valve	Reliability and resilience are functionally equivalent. Classic reliability techniques are applicable and useful.
System (simple)	Fuel pump	
System (complex)	Aircraft	The distinction between reliability and resilience is one of degree. Designers must determine when reliability or resilience is more appropriate. Classic reliability techniques are applicable in specific cases of reliability management; such as the use of FMECA in developing suitable aircraft maintenance plans.
SoS	Air Transportation System or ATS	Reliability and resilience are distinctly different. The definition of SoS reliability is highly context-dependent. Classic reliability techniques based on component reliability must be augmented by additional tools (e.g., robust scheduling of airlines) when managing reliability.

At the component level, measures such as mean time to failure (MTTF, for non-repairable components) and mean time between failure (MTBF, for repairable components), describe in part the reliability of elements. At this level, reliability is an important attribute that drives component design and selection. Components can be designed to minimize the likelihood of a failure, for example by selecting better quality parts, but once a failure occurs, by definition they do not have the inherent ability to survive and recover from the failure. A component can be reliable, but on its own, it cannot be resilient (since it cannot recover on its own), and no additional design guidance can be gained by considering resilience.

The same interpretation can often be applied to simple systems. A fuel pump is reliable if it pumps fuel at the specified rate when required to, and, if it does not pump fuel when not required to. We can for example define a mean time between failures for the pump—though this measure must be defined in the context of some set of possible failure levels (e.g., the pump only provides 95% of the required pressure, vs. the pump fails completely). The fuel pump's reliability is a function of its components' reliability, as

well as its overall design (e.g., use of redundancy). A fuel pump with backup components is designed to be reliable despite failures of its components. As with a component, considering resilience does not provide additional design guidance.

As we consider more complex systems, the context aspect of reliability becomes more important, and the statistical measures become harder to define and interpret. For example, MTBF depends on what level of failure is deemed significant at the aircraft level. So, in the case of an aircraft, we might say the aircraft is 80% reliable, if it is able to conduct a successful flight 80% of the times it is called upon to do so, given nominal operating conditions. An aircraft that must frequently cut missions short or operate at a reduced level due to failures in nominal operating conditions is not reliable. Reliability engineering techniques can be used to identify the sources of this unreliability.

While aircraft engines are designed to be highly reliable, aircraft are also designed to be *resilient* to an engine failure: when an engine fails, the remaining engine(s) compensate for the loss. The engine reliability springs from design, component selection, and a tightly controlled maintenance program that work together to minimize the likelihood of component failure. The aircraft's resilience to engine failure springs from redundant design (the remaining engines provide sufficient thrust to compensate for the loss), protection (the engine cowling is designed to contain most failures, and the engine mountings are designed to fail and release the engine if it presents an unbalanced load), and training (the pilot is trained to shut down a malfunctioning engine and use the aircraft control surfaces to compensate for asymmetric thrust).

Finally, at the SoS-level, reliability and resilience are distinct and highly context-dependent. At this level, reliability is typically some function of the performance of the overall SoS. For instance, we would say that the air transportation network is reliable if some majority of flights arrive and depart as scheduled under some defined set of nominal weather conditions. This reliability is primarily driven by reliable systems (aircraft) and by robust scheduling. On the other hand, the system is *resilient* if it can

continue to deliver passengers to their destination despite rare or unexpected disruptions. The air transportation system is not highly resilient—a large blizzard in one region can disrupt flights around the country for several days. In contrast, some public transportation systems demonstrate higher resilience: when a subway line is unavailable, passengers are transported using buses

2.2.3 Robustness

The terms resilience and *robustness* are often used interchangeably; however, there is an important difference between these concepts. Robustness can be thought of as the property of a system that allows it to satisfy a fixed set of requirements, despite changes in the environment or within the system [Saleh et al., 2009]. While the definition of resilience involves a similar idea, the distinction between the two attributes is that while no performance loss is allowed in the case of robustness, a resilient system may permit a (sometimes temporary) performance loss in "bouncing back" from the adverse event [Haimes, 2009]. Robust systems are expected to satisfy the original performance requirements during a disruption, which may be difficult or costly. Therefore, robust responses are appropriate for a small range of disturbances—those that occur frequently or that can be handled robustly in a cost-efficient manner. Less frequent disturbances, or those that are expensive to respond to without a performance loss, are better responded to in a resilient manner. For example, passenger aircraft are expected to encounter rain and thunderstorms quite frequently. They are therefore designed to be robust to rain, and to fly with enough fuel to be routed around (un)expected thunderstorms encountered en route. In contrast, extreme crosswinds occur less often, and constructing and operating passenger aircraft capable of landing in severe crosswinds is costly. A resilient response is therefore more appropriate. When extreme crosswinds occur, aircraft are diverted to the nearest suitable airport for landing. The passengers and crew are safe, but not at their intended destination, thus in this case the response is resilient, not robust.

2.2.4 Safety

The difference between resilience and safety is quite distinct. Safety refers to the objective of ensuring accident prevention through actions on multiple safety levers, such as technical, organizational, or regulatory [Leveson, 1995; Leveson, 2012; Saleh et al., 2014]. This attribute values human life (or property loss) over other performance traits. Specifically, with respect to resilience, safety can be thought of as the aspect of survivability that is related to minimizing loss of life (or property). In some cases, both these attributes go hand-in-hand. For instance, in the event of a disruption to a transportation system (e.g., a hostile attack on an airport) designers need to plan for both safe (ensuring safety of travelers and employees) and resilient (reduce subsequent delays that occur due to airport closure and redirection of flights to other airports) operations of the SoS. In other cases, such as financial markets and global economies, the emphasis is on performance recovery (e.g.: minimizing fall in stock prices due to shocks to the system). In this case loss of human life (safety) is not a major concern. The above transportation example highlights the role of safety when the system needs to satisfy the same requirements it was designed for (provide transportation services with minimum delay). Safety must also be maintained when other requirements change (though the level of acceptable safety may change). For example, if an aircraft is retrofitted for use as a crop duster, the design must ensure that the pilot is not exposed to the crop dusting chemicals. Thus the retrofitted aircraft must maintain the safe air environment for the pilot.

Safety-critical systems are systems whose “failure might endanger human life, lead to substantial economic loss, or cause extensive environmental damage” [Knight, 2002]. For instance, the flight management system (FMS) on aircraft is a safety-critical system as collects and consolidates important information with respect to radio navigation, geographical positioning, flight planning and the aircraft’s health status. Many SoSs include safety-critical systems at various levels. For example, in addition to the FMS on board an aircraft, the air traffic control system is another safety critical system. Because these systems’ failure can have such negative impacts, there is an entire field of research

and practice devoted to ensuring their safety (see, for example, Bowen and Stavridou [1993] and Storey [1996]).

To summarize, reliability is appropriate when high frequency-low impact disruptions (e.g., rain showers) occur and the SoS (e.g., air transportation system) is expected to maintain functionality without any loss in performance. Robustness is suitable when high (or medium) frequency-moderate impact events (e.g., thunderstorms) occur and the SoS is expected to maintain functionality without any loss in performance (e.g. route aircraft around the thunderstorm). Finally, resilience is appropriate when low frequency-high impact disruptions (e.g., blizzards) occur and the SoS is expected to survive and recover from the adverse event (e.g., divert aircraft to other airports).

2.3 Summary and Conclusions

As discussed earlier, an adequate treatment of SoS resilience should address the following questions:

1. What is resilience in the context of an SoS and when is it appropriate?
    - How can resilience be distinguished from other system-level attributes?
2. How can resilience be designed?
    - What level of resilience is desirable and how resilient is the SoS currently?
    - What principles can be applied to achieve resilience in SoS design?
3. How can resilience be maintained over the SoS lifetime?
    - When does resilience change?
    - How can adverse impacts of changing resilience be observed and mitigated?

This chapter focused on the first question by (1) reviewing how resilience is viewed by different disciplines, and (2) in the case of SoSs, in particular, identifying and characterizing the situations in which resilience is needed. We observe that the essence of this attribute remains constant across the different domains, but the specifics of designing and operating resilient systems varies widely. Focusing on SoSs, we conclude that

considering a spectrum of system-level attributes is useful to enrich overall design and each one adds value in specific ways.

In the next chapter, we take a deeper look designing SoS resilience (the second question). We present an overview of traditional system-level risk and reliability techniques as well as more recent multi-disciplinary approaches that can be applied to SoS resilience.

CHAPTER 3. DESIGNING RESILIENT SoSs: A REVIEW OF METHODS, METRICS, AND CHALLENGES

The focus of this thesis is on supporting the design of resilient SoSs, a vital part of overall resilience management (see). Designing resilience in SoSs consists, on the one hand, of ***evaluating resilience*** (measure, either quantitatively or qualitatively, the resilience of a particular SoS), and, on the other hand, of ***creating resilience*** (determine strategies and features, both technical and non-technical, that can be employed to improve SoS resilience). Since resilience cannot be improved effectively without first measuring it, both these phases are important to overall design and often times need to be analyzed iteratively. In this chapter, we review existing approaches in the literature that can help design resilience. First, we discuss whether and how existing reliability and risk assessment techniques can be leveraged to address SoS resilience. Next, we consider "newer", more multi-disciplinary approaches that have application in the same topic.

3.1 Reliability Engineering and Risk Assessment

Reliability engineering and risk assessment both ask versions of the following four questions [cf., Kaplan and Garrick, 1981]: (1) what can go wrong? (2) how likely is it? (3) what are the consequences? and (4) what can be done about it? Reliability engineering typically focuses on the ability to continue providing some pre-defined functionality despite performance failures, and on quantifying reliability at various levels in the system. Risk assessment considers a slightly different problem, that of operating without causing loss of life or property. Thus in risk assessment the analysis typically begins by attempting to identify all the ways that the system could fail. For example, in air transportation, risks include mid-air collision, or engine failure. Once these risks have

been identified, various approaches can be used to characterize the risks. Here we briefly review some of the techniques used in reliability engineering and risk assessment, and then focus on their application to designing SoS resilience. For more depth on the techniques, the reader is referred to the many excellent texts on reliability engineering and risk assessment (e.g., Rausand and Høyland [2004]).

Hazard identification is one of the hardest parts of risk analysis, because it is not a purely analytical process. Instead it requires a combination of imagination and technical skill. Many approaches to hazard identification have been proposed; most are essentially versions of checklists, which provide the analyst with ideas on what might go wrong [Vaidhyanathan and Venkatasubramianian, 1995; Dunjo et al., 2010]. Hazard identification is difficult in complex systems because the hazards may be largely unknown. There have been attempts to expand the range of hazards to include unknowns (e.g., Paltrinieri et al. [2011]) and several tools have been developed for robust risk analysis to deal with uncertainties (e.g., Ben-Haim [2012] and Cox [2012]). While SoS specific hazard analysis tools have not been developed to date, current techniques can be applied. For example, Robinson [1995] provides an overview of applying HAZOP analysis to electrical power grids and transport systems; Mahnken [2001] describes the use of case studies to identify latent design deficiencies – for instance, best practices from the hazard identification process in the chemical industry can be used to discover flaws in electrical power grids.

Failure modes, effects, (and criticality) analysis (FMEA/FMECA) traditionally considers the impact of component failures on system-level risk. An FMECA analysis begins by identifying the various failure modes of a component (e.g., valve fails open, valve fails shut), and then determines its effects (e.g., coolant not provided), and how critical the failure is to the system (e.g., runaway reaction). FMECAs can be similarly used to identify potential failure modes and to investigate their impact on the overall SoS functionality. Here, each failure is considered individually and independently from other failures, and hence, these techniques will be most helpful for isolated failures in an SoS.

For instance, in the air transportation network, FMECA can be used to assess the impact of individual airport failure modes (e.g., airport closed due to terror alert, or airport closed due to weather) on the overall SoS's capabilities, which in turn could be used to investigate and institute better equipment and procedures at critical airports.

A *fault tree* is a logic diagram that indicates how a system-level failure can be generated by component failures. This analysis begins with an undesirable end state (failure) and then works backwards (deductively) to find which combinations of component failures can result in the end state. An *event tree*, on the other hand, is a logic diagram that allows designers to systematically study the propagation of a basic initiating event to its potential consequences. Event trees are almost the reverse of fault trees in that they work forward (inductively) from an initiating event and develop a time-sequence of events to determine which, if any, undesirable end states can be reached from the initiating event [Rasmussen, 1975]. Although their application to (and, in particular, quantification) complex systems is challenging (see Siu, 1994), fault and event trees can be used in SoS resilience analysis to document how system failures can combine to decrease SoS performance (e.g., Fleming et al. [2013]).

Because SoSs are particularly susceptible to common cause failures and partial failures, we believe that fault and event trees do not serve well to assess probabilities of failures. Similarly, other tools for quantifying failure probabilities, such as Bayesian-based statistics [Clemen and Winkler, 1999], whether based on system or component level data, are also harder to apply to complex systems and SoS involving a combination of hardware, software, and people [Aven, 2013a]. Here, as in hazard identification, new or complex systems are especially challenging. For example, over its lifetime, assessments of Space Shuttle reliability ranged from 1 in 100 to 1 in 100,000 [Feynman, 1986]. When systems must operate in a wide range of, or poorly understood, environments, risk quantification becomes even more difficult. For example, because the risk of earthquakes in the US Northeast was underestimated in the 1970s, nuclear power plants in the region actually have the highest risk of seismic damage [Dedman, 2011].

Recent research efforts have attempted to adapt some "traditional" reliability engineering methods, such as *Bayesian belief networks (BBN)* and component importance measures, to networks of complex systems. BBNs are directed acyclic graphs used to illustrate the relationships between system failures and their causes or contributing factors. BBNs are considered to perform better than fault trees at reliability analyses since they are not limited to binary events and can handle partial failures. For example, Weber and Jouffe [2006] formalize a method using Dynamic Bayesian Networks to model the reliability of manufacturing processes. Their focus on the flows between systems highlights key dependencies and common failure modes. This Bayesian approach can potentially be applied to the design of interdependencies in SoSs.

Component-failure based reliability and risk techniques typically suggest using higher reliability components or redundancy to improve system-level reliability. While some SoS systems can be made more reliable (e.g., more reliable aircraft), the extent of possible improvement is often limited (e.g., we can provide snow-clearing at an airport, but during a blizzard the airport will have to shut down for safety reasons). Also, given the heterogeneity and, often wide geographic distribution, of the constituent systems, redundant systems in an SoS are impractical and costly. Using redundancy alone runs the risk of overlooking other, more optimal, resilience improvement measures. Section 3.2.1 highlights some alternative techniques to creating resilience in SoSs.

Some recent research has acknowledged the limitations of the direct application of existing reliability techniques and offered ways to expand these methods for the useful analysis of SoS resilience [Johansson et al., 2013; Zio and Ferrario, 2013]. For example, Zio and Ferrario [2013] apply an extension of existing reliability analysis using Monte-Carlo simulations to assess the seismic risk for a nuclear power plant embedded in the power, water, and transportation networks that support its operation.

In summary, reliability and risk-based approaches to resilience in SoS do have application, but their use can also lead to incorrect assessments of resilience (see Table 3.1). Park et al. [2013] suggest that the lack of progress on resilience engineering in SoS

may be "partly because quantitative design approaches consistent with principles of resilience remain elusive, and partly because analytic approaches to resilience in engineering have become conflated with existing approaches to analysis of risk".

Table 3.1 SoS resilience design guidance provided by traditional reliability and risk assessment techniques

Reliability and Risk Assessment Method	Design questions addressed by method (wholly or partially)	Limitations with respect to SoS design
FMEA/FMECA	• How can resilience be created? • When are specific resilience improvement strategies suitable?	• Focus is on single component failures and hence cannot capture cascading failures due to interdependencies prevalent in SoSs • Typically deal with hardware component failures and cannot capture crucial software and organizational interdependencies inherent in SoSs
Fault and event trees	• How can resilience be created? • When are specific resilience improvement strategies suitable?	• Deal with binary failures – cannot handle partial failures as are often times seen in SoSs • Can result in large and complicated documentation – making them less likely to be useful for design guidance • Does not provide specific insight on design improvement
Bayesian belief networks	• Where (in the SoS) should resilience improvement strategies be incorporated?	• Depends on quality and extent of prior beliefs (excessive optimistic or pessimistic expectation can distort results)
Component importance measures	• Where (in the SoS) should resilience improvement strategies be incorporated?	• Consider binary failures – cannot handle partial failures • Assume system architecture is fixed – not applicable in case of SoSs where network is constantly evolving
Probabilistic risk assessment	• How can resilience be measured?	• Requires near-complete identification of hazards (disruptions) • Does not provide specific insight on design improvement

3.2 SoS-focused Approaches

Other than suggesting reduction of failure rates (e.g., through better components, or more frequent maintenance), reliability and risk analysis methods do not provide guidance on other types of mitigation strategies. As a result, in many cases, resilience is achieved through a trial-and-error process rather than through detailed SoS-level analysis. Such ad-hoc approaches could result in achieving too much (unused) resilience in one part of the network, and too little resilience in another. Also, such approaches could make an SoS highly resilient to certain kinds of disruptions but less resilient to other threats. To design and test for resilience across a broad range of conditions requires understanding at a much finer-grained level how the systems will be used, the environments in which they will be used, and the threats they can expect to encounter [Neches and Madni, 2012]. This view echoes that of researchers who raise the need for a different perspective of resilience in the context of SoSs [Sheard and Mostahari, 2008; Madni and Jackson, 2009; Georger et al., 2014].

This section draws on a variety of "newer" research efforts to provide a sense of how SoS resilience can be evaluated and created. We broadly categorize these studies into a set of three design approaches: principles, tools and models, and metrics (see Table 3.2), and highlight how useful they are in providing specific design guidance.

Table 3.2 Design guidance provided by SoS-focused design approaches

Design Approaches	**Design questions addressed by method (wholly or partially)**
Design principles	• How can resilience be created? • When are specific resilience improvement strategies suitable? • What are the tradeoffs associated with these strategies?
Simulation tools and models	• How can resilience be created? • When are specific resilience improvement strategies suitable? • Where (in the SoS) should these strategies be incorporated?
Metrics and frameworks	• How can resilience be measured? • When is the SoS resilient enough?

3.2.1 Design Principles

A design principle, or heuristic, is an abstraction of experience that can be used to effectively guide engineering design [cf. Maier and Rechtin, 2000]. For example, in systems engineering, one design principle is to minimize coupling, which can, for example, be accomplished by increasing the modularity of the design. Ensuring stable, intermediate forms during SoS development and evolution is a principle applicable at the SoS level (see Maier and Rechtin [2000] for a list of heuristics pertinent to architecting SoS). Here, we present a set of ten principles to guide the design of SoS-level resilience. Although this list is not intended to be exhaustive, we believe many resilience improvement strategies derive from these principles. While several of the principles outlined below are rooted in systems engineering (see Jackson and Ferris [2013] for a recent compilation), the relevant principles have been adopted here for SoS design guidance[2]. The list is organized by theme as follows: the first four principles represent system-level design features; the next two represent network-level design features; the following three are based on human involvement (observation, decision-making, communication); and the last principle suggests a combination of the previous nine.

1. Physical redundancy. Employ redundant hardware (backups) to provide functionality when primary systems in the SoS fail [Jackson and Ferris, 2013]. For example, in the case of a public transportation network, one way to create physical redundancy is by maintaining extra buses at city depots. In the event of a disruption (e.g., traffic jam or an accident) these spare buses could be used on the original routes in place of the failed primary buses, or depending on the situation, they could even be used to augment service by running different routes.

2. Stand-in/Functional redundancy. Leverage heterogeneity in the SoS to provide redundancy without adding additional systems [Zhang and Lin, 2010; Jackson and Ferris, 2013; Uday and Marais, 2013]. For example, loss of the LCS (see Figure 1.1) can be

[2] We do not explicitly consider cyber resilience here. Though cyber resilience is increasingly becoming an integral concern for these SoSs, principles that achieve this resilience require a different, more software-centric approach

compensated for by using better-equipped helicopters (carrying more weapons and larger fuel tanks) and improved unmanned surface vehicles (sophisticated surface imaging and radar capabilities). The enhanced features on the helicopters and surface vehicles allow these systems to be re-tasked to perform new functions in the event of an LCS incapacitation.

3. System-level Properties. Improve system-level properties, such as flexibility, robustness, and adaptability, of the constituent systems to achieve SoS-level resilience. For example, flood protection (***robust design***) at entrances to subway stations in large cities can prevent flooding during extreme disruptions such as hurricanes, thereby preventing catastrophic repercussions to the rest of the transportation infrastructure [Higgins, 2012]. Another way to improve resilience at the regional transportation level is by enabling ***flexibility*** at the lowest service level (e.g., through the use of larger buses).

4. Repairability. Decrease total time to recovery, that is, ensure availability of adequate resources and personnel to limit disruption impact on the primary failed system [Jackson and Ferris, 2013]. For example, if a blizzard occurs at an airport, while closure of the facility is inevitable, having appropriate snow removal equipment, trained personnel, and instrumentation capabilities, can provide expedited recovery as the storm's impact weakens. The repairability principle can also be applied at the system level in order to have SoS level benefits. For instance, if the primary radar at an airport fails, timely repair of this system will ensure speedy return to full service of both terminal and en-route operations.

5. Inter-node Interaction. Every node in the SoS should be capable of communicating, collaborating, and coordinating with every other node [Jackson and Ferris, 2013]. For example, in the event of a hostile attack that results in the loss of an LCS (see Figure 1.1), other systems in the SoS, especially those that draw from or provide information to the ship, must be immediately aware of its incapacitation. This can be achieved by improving the communication capabilities between the systems in the SoS.

6. Localized capacity. If a single node in the SoS is damaged or destroyed, the remaining nodes should continue to function [Jackson and Ferris, 2013], that is, cascading failures should be prevented or minimized. For example, if an airport closes, having alternative airports with adequate capacity nearby will allow flights to be diverted, while minimizing the domino effect through the rest of the airspace.

7. Human-in-the-loop. Humans should be in the loop when there is a need for "rapid cognition" and creative option generation [Madni and Jackson, 2009]. For example, the blackout across the Northeast in 2003 happened in part due to cascading automatic failures: preset relays were programmed to protect individual equipment, and as each one acted, isolating a power line or a transformer, the cascading disturbance caused a massive blackout impacting hospitals, airports, and subways [Wald, 2013].

8. Drift correction. Pre-emptively initiate resilience measures before the disruption so that mitigation steps may be initiated before the onset of the actual adverse event [Jackson and Ferris, 2013]. For instance, in the aftermath of the Icelandic volcano in 2010 that had widespread impact on global aviation services, sensors are being developed to provide warning of volcanic ash and to provide pilots with real-time information to alter their flight paths [BBC, 2010].

9. Improved communication at organizational level. Facilitate real-time information sharing and command and control activities between stakeholders and operators [Chang et al., 2013]. Improved communication at the organizational level can minimize confusion and mismanagement in the aftermath of a disruption. For example, in the event of a terror attack at an airport, timely and effective sharing of information regarding recovery procedures between regulatory authorities, airports, and airlines, can help minimize performance impacts on the larger network: passengers can be evacuated safely and re-directed to other modes of transport efficiently.

10. Layered defence: Use a combination of the above design principles to balance protection (disruption prevention) and resilience (surviving and recovering from a disruption) in SoSs [Haimes et al., 2008].

Table 3.3 highlights which region of the resilience curve (survivability and recoverability) each design principle addresses.

Table 3.3 Resilience improvement implications of design principles

Category	Design Principles	Resilience Improvement			
		Improve survivability	**Improve mitigation capability**	**Improve/ facilitate mitigation accessibility**	**Reduce time taken to restore disrupted systems**
System-level	1. Physical redundancy		✓		
	2. Functional redundancy		✓		
	3. System-level properties	✓			
	4. Repairability				✓
Network-level	5. Inter-node interaction			✓	
	6. Localized capacity	✓			
Human aspects	7. Human-in-the-loop	✓		✓	
	8. Drift correction	✓			
	9. Improved communication	✓		✓	
All levels	10. Layered defense	✓	✓	✓	✓

3.2.2 Simulation Tools and Models

Improved computational capabilities in recent decades have led to the development of high-fidelity simulations and models. These tools can aid the design process in several ways; for example, simulations can help study failure propagation, evaluate different recovery strategies, and identify critical nodes and links. While we can leverage existing network theory based models to analyze links and nodes in SoSs, many of these methods assume homogenous nodes, leading to difficulties in capturing key SoS characteristics such as diversity and interdependencies. Given the inherent complexity of SoSs, efforts are needed to build on these network-based models by harnessing multiple fields such as control theory, statistical analysis, and operations research. Researchers have in recent years begun to address these issues and here we review efforts on relevant and useful simulation tools.

Failure Propagation. Understanding how disruptive impacts propagate is an important element of any resilience analysis, especially in the case of SoSs where the coupling between independent systems is not always evident. Failure propagation models are useful to identify critical links and to assess recovery options. Such models can be used, for example to the air transportation system to identify critical airports and to assess recovery options (road, rail, and air) if services at these airports fail.

Most resilience-related research uses some aspect of network theory to study effects of disruptions [Crucitti et al., 2004; Ash and Newth, 2007; Kurant and Thiran, 2007; Ulieru, 2007; Reed et al., 2009; Buldyrev et al., 2010; Sterbenz et al., 2011]. With many SoSs, the assumption of homogenous nodes is not justified as these networks typically consist of heterogeneous nodes (each performing different functions). A few studies have considered nodes with the same function but different capacities [Motter and Lai, 2002; Crucitti et al, 2004].

Instead, multi-layer networks resilience is gaining increasing attention as a better way to represent heterogeneous networks [Castet and Saleh, 2013]. Networks can be modeled as

multi-layers in two different ways. First, the network may consist of different physical layers. For example, the transportation system can be modeled as a road layer, a rail layer, and so forth. Or a network may require support from different layers. For example, the rail network depends on the electricity network. Research in this field has led to the introduction of interdependent network analyses to characterize the properties of such networks [Rinaldi, 2004; Newman et al., 2005; Kurant and Thiran, 2007; Xu et al., 2011; Ouyang, 2012; Trucco et al., 2012; Filippini and Silva, 2013]. Applying these studies to SoSs, designers can study how a failure in one network can have repercussions in the other and how interdependent networks can fail catastrophically after the removal of a small fraction of nodes. These results in turn can guide resource allocation at critical nodes. For example, in a multi-modal transportation network, impacts of disruptive events can be avoided by co-locating certain subway and bus stations thereby providing redundancy for the two transportation modes.

Apart from network theoretic approaches, recent research has attempted to leverage control theory to deal with resilience of interconnected and interdependent systems (e.g. Barabási and Albert [1999], Liu et al. [2011], and Alessandri and Filippini [2013]). For instance, with the ultimate goal of developing resilient controllers, Alessandri and Filippini [2013] present an initial framework that uses switching linear dynamics to cope with nominal and off-nominal (failure) behavior of interconnected systems.

Recovery Strategies. Simulation tools can (1) allow designers to study a range of resilience improvement options, (2) facilitate in-depth studies by allowing a large number of parameters to be varied, and (3) usually provide some visual representation of design implications that is vital to stakeholder communication. Most of these tools have been developed for infrastructure networks, and can be applied to other SoSs relatively easily [Bruneau and Reinhorn, 2004; Shinozuka et al., 2004; Miles and Chang, 2006; Zobel, 2011; Barker et al., 2013; Barker and Baroud, 2014]. For example, Shinozuka et al. [2004] developed several restoration curves to study the return of electric power and water supply to customers after major catastrophic events, such as earthquakes. Similarly, Miles

and Chang [2006] developed a simulation tool that generates recovery paths for communities in the aftermath of a disaster.

Critical Nodes and Links. Mathematical models and simulations can help designers identify resilience-based regions of concern (critical nodes and links) within SoSs [Garvey and Pinto, 2009; Guarniello and DeLaurentis, 2013]. Guarniello and DeLaurentis [2013] use the Functional Dependency Network Analysis model (originally proposed by Garvey and Pinto, 2009) to identify critical systems in SoSs and critical dependencies between constituent systems. For instance, in the naval warfare SoS, disruption of the LCS could lead to incapacitation of the weapons-equipped helicopter since the LCS is now unable to transmit crucial target information to the airborne system.

3.2.3 Metrics and Frameworks

Measuring resilience is a key component of designing resilience (see Figure 1.2**Error! Reference source not found.**): quantitative assessment techniques are needed to evaluate the effectiveness of and to compare various resilience improvement designs. While metrics and frameworks add significant value to the SoS analyst's toolkit, developing generalizable measurements that can be applied broadly across a wide range of different SoSs is challenging. Additionally, given the diversity of stakeholders associated with SoSs, difficulties arise with capturing all aspects of interest such as cost, performance, and safety, in a resilience metric. In this section, we review various metrics and frameworks.

Metrics. Ayyub [2014] proposes a resilience metric that is a function of the failure profile, recovery profile, as well as the various times involved with resilience, such as time of disruption, time during of failure, and time duration of recovery. Henry and Ramirez-Marquez [2012] define resilience as a ratio of system recovery to the loss after a disruption, where recovery and loss are measured as changes with respect to SoS performance. Francis and Bekera [2014] develop a resilience factor that is a function of

speed of recovery and the various performance levels before and after the disruption and recovery actions. These metrics can be used to estimate the overall resilience of different SoS designs. For example, military operators can adopt these metrics to perform analyses of alternatives – should target identification for a mission be provided using satellites or UAVs? And, which SoS architecture would be most resilient to known and unknown threats? Richards [2009] presents an overall resilience metric that is a measure of the system utlility over the design life. While useful to make an overall comparison of different systems, such a measure provides little design guidance regarding resilience improvement.

While there are "advantages to using a single calculated value to define resilience, it is also important to recognize the potential issues associated with doing so" [Zobel, 2011]. In particular, an overall metric provides little, if any, information regarding specific areas within the SoS that need attention. Also, in the context of SoSs, the uncertainties associated with network operations, evolution, and management are quite large and hence one metric may not be able to capture all the unknowns. To address these concerns, some studies focus on capturing or disentangling the various dimensions of resilience. For example, Barker et al. [2013] developed two resilience-based component importance measures for networks. Their study quantifies the impact of a link disruption on overall resilience, as well as the impact when a link cannot be disrupted. Han et al. [2012] propose a conditional resilience metric using Bayesian networks to measure each constituent system's contribution, and subsequently to identify the most critical systems to the overall SoS resilience. Pant et al. [2013] use an extension of the economic input-output model to investigate the resilience of interdependent infrastructures. They develop two metrics: *static economic resilience*, which focuses on the survivability aspect of the overall network, and *dynamic economic resilience*, which includes the recovery of the network after a disruption. There have been a few attempts to modify and/or expand existing component importance measures to analyze the resilience of networks. For example, a recent paper (Barker et al., 2013) develops two resilience-based CIMs for networks. Although this study does consider the resilience of the overall network, the

analysis and subsequent metrics are only applicable to networks with homogenous nodes. In addition, emphasis is placed on network flow (that is link resilience) rather than to nodes. While this approach may be beneficial in addressing network resilience, it appears to be useful only for networks where the flow between mostly similar nodes is of concern rather than the particular functions carried out at the nodes themselves.

Frameworks. Frameworks have been the dominant trend in urban infrastructure resilience research. For example, the Multidisciplinary Center for Earthquake Engineering Research (MCEER) at the State University of New York views resilience as a combination of four 'R's: robustness, redundancy, resourcefulness, and rapidity, and proposes a framework to measure each 'R' [Bruneau et al., 2003; Shinozuka, 2004]. Other work that has emerged from MCEER suggests a resilience index between 0 and 1 for each infrastructure network and then proposes a technique to aggregate all the indexes for an overall resilience measure [Renschler et al., 2010]. Similar efforts at Carnegie-Mellon's Software Engineering Institute have resulted in a Resiliency Engineering Framework (REF), which posits a vector of 21 capability areas that can be used to score the resilience of cyber services [SEI, 2009]. While most of these frameworks do consider, to a certain degree, the stochastic (uncertain) nature of inputs, the data needed for resilience studies are in most cases limited and incomplete. To handle these issues, Attoh-Okine et al. (2009) present a method to construct resilience index for urban infrastructure using belief functions that are capable of handling imprecise and subjective information

3.3 Summary and Conclusions

Returning to the broader context of this research, the following are the main questions that need to be addressed by any comprehensive resilience management plan:

1. What is resilience in the context of an SoS and when is it appropriate?
    - How can resilience be distinguished from other system-level attributes?
2. How can resilience be designed?
    - What level of resilience is desirable and how resilient is the SoS currently?
    - What principles can be applied to achieve resilience in SoS design?

3. How can resilience be maintained over the SoS lifetime?
    - When does resilience change?
    - How can adverse impacts of changing resilience be observed and mitigated?

In this chapter, we began to answer the second question and discussed methods in the literature that can be applied to addressing SoS resilience. Major limitations of the metrics and techniques in the context of SoSs include:

- **Binary characterizations of system states:** Most analyses compute network wide impacts by assuming systems and links are either failed or operational.
- **Lack of focus on the recovery:** Most studies focus on the impact of system and link failures on network level performance metrics with little consideration of active recovery strategies.
- **Lack of design guidance:** Aggregated metrics at the network level provide little information on how SoS design can be improved in the context of resilience.

An alternative approach to SoS resilience design that addresses these limitations is presented in the next chapter.

CHAPTER 4. A NEW APPROACH TO RESILIENCE DESIGN: SYSTEM IMPORTANCE MEASURES

This chapter introduces a new approach to resilience design that is applicable to systems-of-systems. The proposed approach provides specific SoS design guidance by identifying **where** in the SoS resources need to be targeted to improve the overall resilience and determining **how** the improvements can be realized.

As mentioned in the previous chapter, employing a single metric to evaluate SoS resilience provides little direct design guidance. Such a metric provides little, if any, information regarding specific areas within the SoS that need attention or specific aspects of the SoS's resilience that could be improved. Also, a single metric does not provide guidance on which SoS should be changed and how it should be changed. In this work, we present one approach that can enable more effective and informed decision-making in the context of SoS resilience improvement.

4.1 Component Importance Measures: Motivating the SIM Approach

At the system level, researchers have developed a set of metrics, collectively known as Component Importance Measures, to rank constituent components based on their impact on the system level risk and/or reliability. CIMs are well established within reliability engineering and risk assessment [Elsayed, 1996; Van der Borst and Schoonakker, 2001; Rausand and Høyland, 2004; Ramirez-Marquez and Coit, 2007]. Traditionally, component importance measures have been used to identify and evaluate the impact that disruptions at the component level have at the system level. In particular, CIMs allow practitioners to rank components based on the order in which they impact the system.

Typically, importance measures follow two steps: (1) quantify the effect of individual component reliabilities (or lack thereof) on the system, and, (2) rank the components in terms of their relative importance to system-level reliability. Table 4.1 summarizes some commonly used component importance measures. Note that component ranking may vary depending on the importance measure used.

Table 4.1 Component Importance Measures (CIMs)

CIM	Question answered by CIM	CIM Equation
Birnbaum importance	What is the reliability importance of component *i*?	$I_i^B = S_R - S_R(i=0)$
Improvement potential	What is the improvement in system reliability when component *i* is replaced by perfect component?	$I_i^{IP} = S_R(i=1) - S_R$
Risk Achievement Worth (RAW)	What is the increase in risk/decrease in reliability if component *i* fails?	$I_i^{RAW} = \frac{1 - S_R(i=0)}{1 - S_R}$
Risk Reduction Worth (RRW)	What is the decrease in risk/increase in reliability if component *i* is replaced by perfect component?	$I_i^{RRW} = \frac{1 - S_R}{1 - S_R(i=1)}$
Fussell-Vesely	What is the fractional contribution of component *i* to the risk/reliability?	$I_i^{FV} = \frac{S_R(i=1) - S_R}{1 - S_R}$
Criticality importance	What is the probability component *i* has failed given system has failed, i.e., probability that component *i* has caused system failure?	$I_i^{CR} = I_i^B \cdot \frac{1 - p_i}{1 - S_R}$

Note: S_R = System reliability (baseline); $S_R(i=1)$ = System reliability when component *i* is replaced by perfectly reliable version of itself; $S_R(i=0)$ = System reliability when component *i* fails; p_i = Reliability of component *i*

Can component importance measures be employed as-is to study the importance of systems in SoSs? To answer this question, we consider a few underlying assumptions of these measures: (1) components are either failed or working, (2) the structure of the system is fixed and does not evolve with time, and, (3) components are independent. Reflecting on the earlier discussion on reliability and resilience, we conclude that these measures do not capture the survivability and recoverability aspects of continually

evolving SoSs. Additionally, component reliability can be estimated relatively easily, while SoS resilience is a more nuanced entity that in many cases is a non-linear function of, at the very least, two attributes: performance and time.

Our research focuses on developing importance measures specifically for systems-of-systems that are characterized by diversity in nodes and functions. Similar to the CIMs described above, system importance measures help identify and rank systems in an SoS that have the most impact on different aspects of the overall resilience.

This work presents three System Importance Measures (SIMs) that rank or prioritize the constituent systems of an SoS based on their *resilience significance*. We say that a system is *resilience significant* if a disruption of the system contributes significantly to measures of SoS performance. As will be explained in this chapter, these measures are an aid to design in that they help determine "where" in the SoS resources need to be targeted so that they provide the most benefit in the event of disruptions.

Figure 4.1 provides an overview of the SIM-based resilience design process. This approach uses an iterative process to determine promising design choices. First, baseline SoS resilience is **evaluated** using system importance measures (SIMs). The outcome of this stage is a resilience map that indicates the relative resilience significance of systems within the SoS. In the second stage, SoS resilience is **improved** using appropriate strategies from a list of design principles. Now, the new SoS designs can be re-evaluated using the SIMs to determine whether the chosen strategies have been effective in addressing the concerns (significant systems) identified in the first step. Based on the specific needs of an SoS, decision-makers can iterate between the two steps to find a set of practical and effective design improvements.

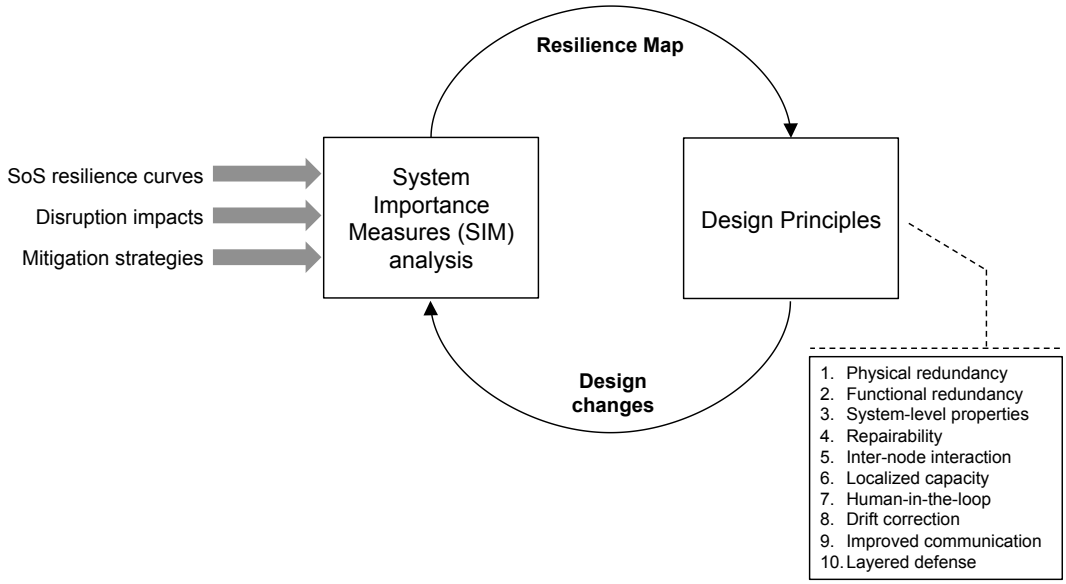

Figure 4.1 A New Approach to SoS Resilience Design

Specifically, the resilience design process comprises four phases (see Table 4.2). The first three phases constitute the SIM analysis where current SoS resilience is evaluated: Phase 1 – what can go wrong?; Phase 2 – what are the consequences?; and Phase 3 – what is the current resilience of the SoS? The outcome of third phase is a resilience map that summarizes how well or how badly the SoS currently handles disruptions. The last phase (Phase 4) is SoS design improvement and asks: What can be done to increase resilience of the overall SoS? The outcome of this phase is a set of design changes.

Table 4.2 Four phases in SIM-based SoS Resilience Design

Phase	Task	Stage
1	**Identify potential disruptions.** What can go wrong?	**SIM Analysis**
2	**Determine impacts of disruptions.** What are the consequences of unmitigated disruptions?	
3	**Determine current resilience of SoS.** How well is the current SoS able to handle the disruptive impacts?	
4	**Determine design modifications to improve resilience.** What can be done to improve SoS resilience?	**Application of Design Principles**

Classic risk-based design involves answering the following questions: What can go wrong?; What are the consequences; and, What can be done about it? While the SIM-based resilience design process follows a similar course (see Figure 4.2), we incorporate features within the original design process that are specific to SoSs. For instance, we present (1) SIMs to evaluate the consequences of adverse impacts on the SoS and (2) design principles that leverage SoS characteristics to suggest suitable design improvements. The SIMs focus on understanding SoS-level impacts of disruptions and on pointing to potential design improvements, and hence can subsequently be used in cost-benefit analyses to determine which improvements can be implemented.

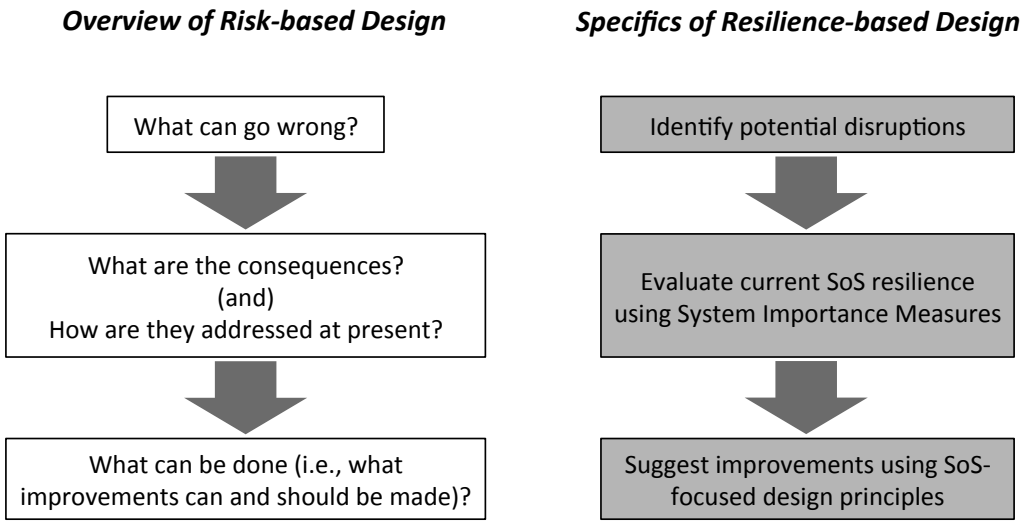

Figure 4.2 Distinguishing features of Resilience-based design within the context of Risk-based design

The purpose of the SIM-based resilience design method is to aid decision-making at the design stage and during operations. During design, the SIMs can be used to identify resilience gaps and possible solutions. During operations, the SIMs can be used to choose the most appropriate response to a disruption. For example, a resilience design might include adding both bigger buses and a backup bus. Then, during operations, the SIMs can be used to select the most appropriate response based on the particular disruption.

We begin with the identification of potential disruptions, followed by an evaluation of how well the SoS currently handles these adverse impacts, and finally determine design changes that can improve resilience. So, while resilience is witnessed at the operational level (how does the SoS survive and recover from disruptive impacts?), the intent of the proposed approach is to facilitate design-related decisions, the results of which have implications for SoS operations.

4.1.1 Simple illustrative SoS

We use an illustrative example in this chapter to highlight key outcomes of each of the four phases (see Figure 4.3). This SoS is a much-simplified version of an urban transportation network and has been chosen for ease of explanation. The SoS, comprising three systems (a bus, a subway, and a ferry), enables transportation of passengers from A to B. Thus, the overall capability of this simple SoS is the movement of people from A to B.

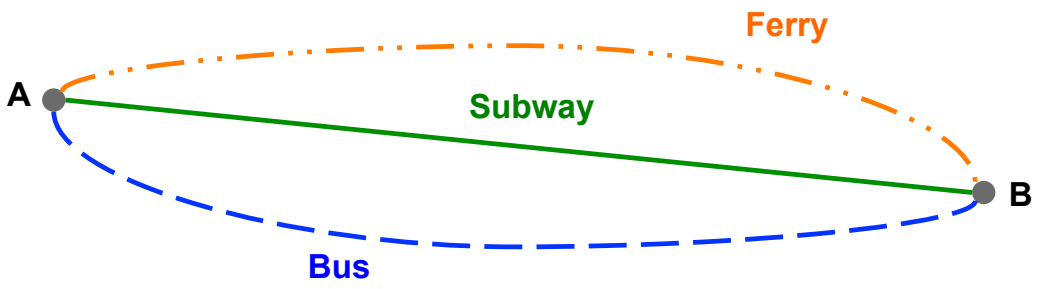

Figure 4.3 Illustrative example SoS

There are many different ways to describe SoS performance. For instance, in urban transportation SoSs, measures of interest include average delay, frequency of service, demand, and vehicle throughput. Also, the various modes of transportation serve different types of passengers with different preferences. Thus, the utility of an SoS is driven by a range of performance measures and stakeholder preferences. In addition, as shown in Figure 4.2, it is also necessary to consider the cost of making improvements. Chapter 6 discusses some potential ways of incorporating SIMs into cost-benefit analyses.

For ease of explanation of the resilience design process we define SoS performance of the illustrative example as the number of passengers (passenger ridership) transported between A and B, and we do not consider the cost of mitigations.

4.2 Identify Potential Disruptions (Phase 1)

A *disruption* is an event that can interrupt some activity or process. With respect to SoSs, we define disruptions as events that adversely impact the overall SoS performance. *Instigating events* cause disruptions. For example, in the case of a military operation, a disruption is the inability of the ship to fire its own weapons due to an attack by an enemy agent. Here, the attack on the ship is the instigating event. Another example of a disruption is the closure of an airport, such as O'Hare International (ORD), due to some adverse weather situation (e.g. snowstorm in Chicago). The instigating event here is the snowstorm.

Typically a disruption definition consists of three parts (see Figure 4.4): impact of the disruption (at the SoS-level), likelihood of the disruption, and cause (instigating event) of the disruption. In the previous example, closure of the airport is the *disruption*, the storm is the *instigating event,* the frequency of such closures is the *likelihood*, and delays and flight cancellations are *impacts*.

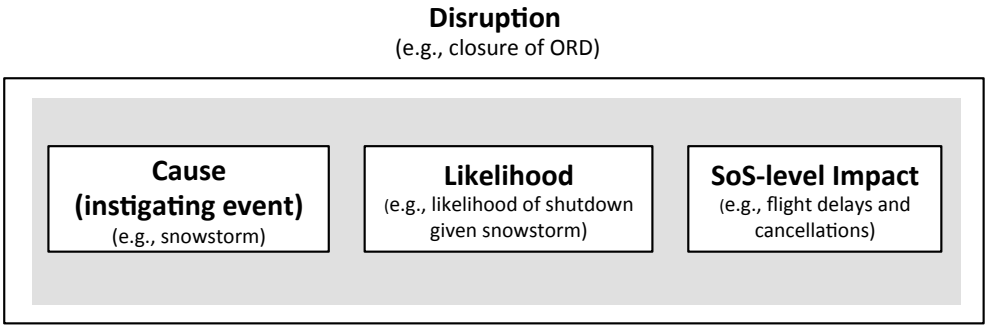

Figure 4.4 Defining a single-system disruption

Instigating events can also cause multi-system disruptions. We term these events as common cause disruptions. For instance, a snowstorm (instigating event) in the New York region can cause the disruption of the three major airports in the area – John F. Kennedy International Airport (JFK), LaGuardia Airport (LGA), and Newark Liberty International Airport (EWR) (see Figure 4.5). The SoS-level impact is the total impact of the three airport closures. The overall likelihood of this multi-airport disruption is a function of the three individual likelihoods given a snowstorm.

Multi-system disruptions can also occur when disruptive impacts propagate through the SoS with systems failing in sequence (see Rinaldi et al. [2001]). These events are called cascading disruptions.

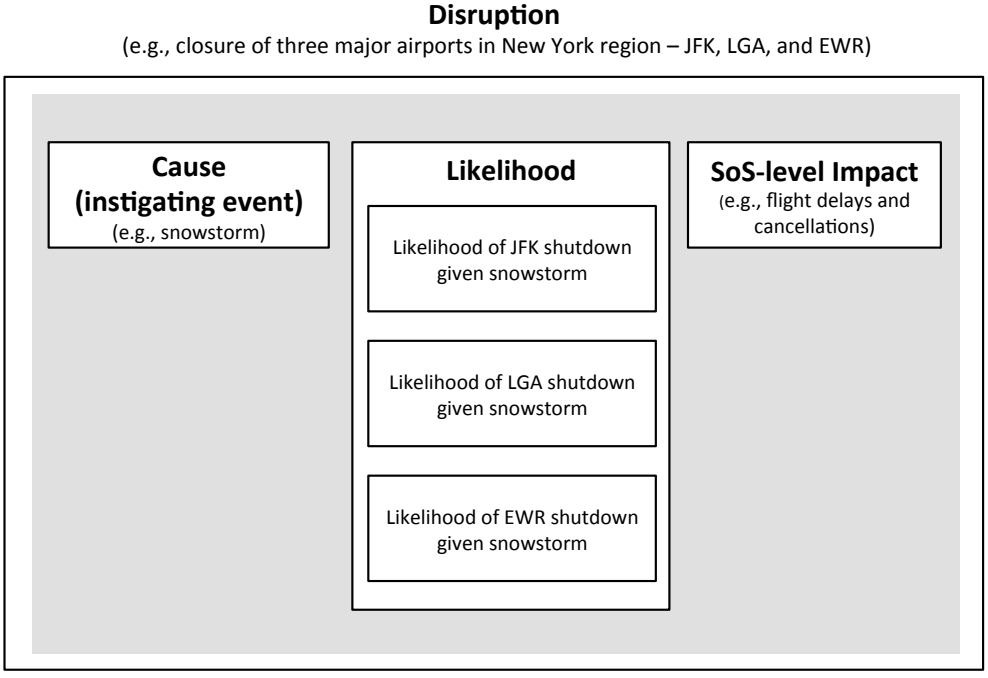

Figure 4.5 Defining multi-system disruptions

In this research we are primarily concerned with the impact (described in Chapters 4 and 5) and likelihood (discussed in Section 6.1.4) of disruptions. In many cases, such as adverse weather events, decision-makers have more control over the response of the SoS

to disruptions than over the instigating events (causes). As a result, focusing on the impacts and likelihood of the disruptions rather than the causes may often be more useful in terms of planning and resource allocation.

Returning to the air transportation SoS, examples of disruptions include closure of ORD (due to a snowstorm), reduced capacity at JFK (due to unanticipated closure of a runway), and shutdown of ATL (due to a terrorist threat). Using suitable simulation tools and models, SoS-level impacts of these disruptions can be evaluated. Chapter 5 discusses some of these tools.

Determining the likelihood of disruptions is relatively harder; such estimates need careful consideration of multiple factors such as frequency of disruptive events, forecasts of service demand, architecture of the SoS (e.g., interdependencies that can cause cascading failures), and SoS evolution. When the potential disruptions are known a priori (e.g., winter blizzards in the north east US typically occur every year), historical data can be leveraged to estimate disruption likelihoods. For example, Figure 4.6 was generated using historical data and points to the amount of snow that leads to school closings in different regions of the US [Barkhorn, 2014]. In the case of unanticipated disruptions, although the causes may be hard to predict, research has shown that their likelihoods can be estimated by leveraging subjective estimates by experts (see, for example, Okashah and Goldwater [1994]).

In summary, while it is practically impossible to predict all adverse events or scenarios for any SoS, a thorough analysis of disruptive impacts and mitigations can be used to handle whole classes of potentially disruptive events.

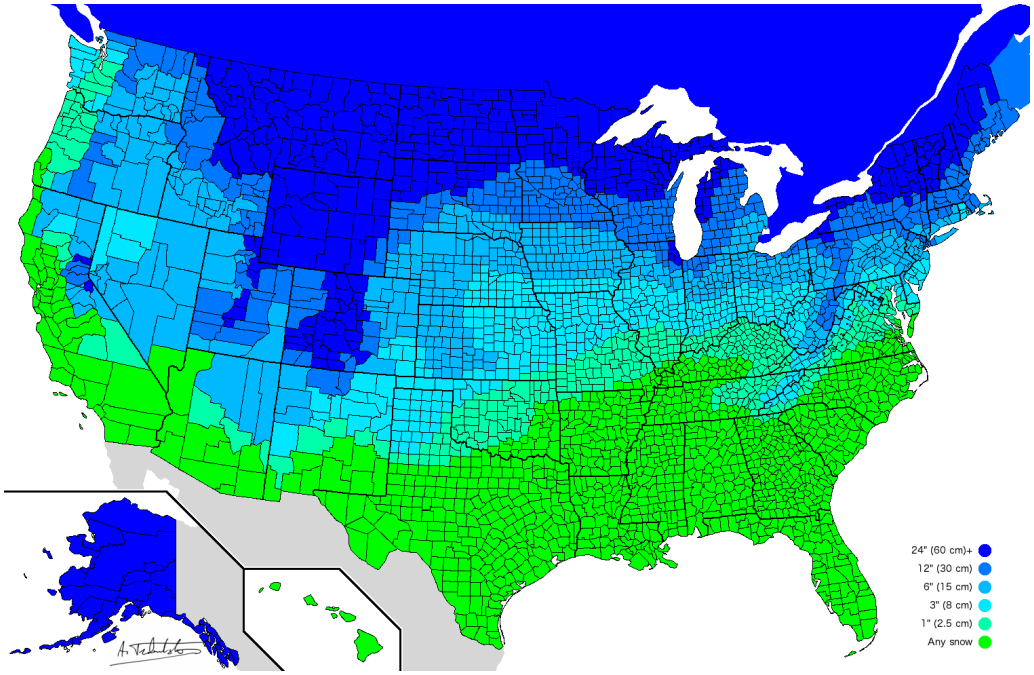

Figure 4.6 Amount of snow needed to close schools in the US [Barkhorn, 2014]

Vulnerability maps are useful tools to qualitatively represent the likelihood and impact of different disruptions for a particular SoS [Sheffi and Rice, 2005]. An example is shown in Figure 4.7. Analysts and decision-makers can place various threats in the appropriate quadrant of the vulnerability framework. However, it must be noted that these maps are not static – they must be continually monitored as, in time, new threats may emerge and the positions of existing disruptive events can change. For example, cyber-attacks on infrastructure SoSs used to be rare, but more recently the likelihood of these threats has increased.

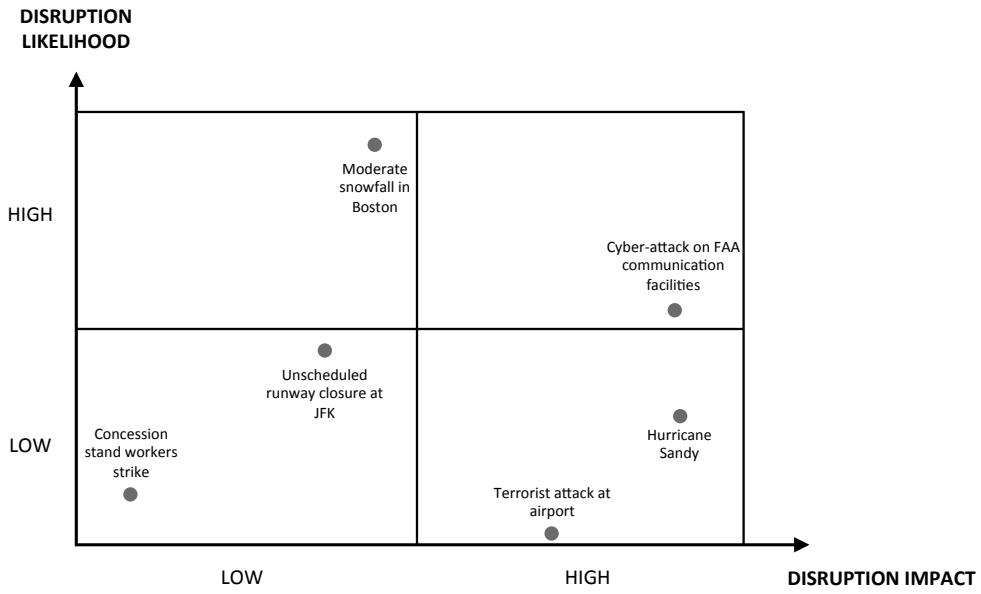

Figure 4.7 Vulnerability map (showing selected disruptions) for air transportation network in North-East Corridor

4.2.1 Outcome of Phase 1

The outcome of Phase 1 is a set of potential disruptions of the SoS. The task of identifying potential disruptions can be carried out by a team of analysts using relevant methods such as brainstorming in a group setting and by leveraging historical data (e.g. age of vehicles, maintenance data, weather information, policy changes). This step is similar to the first phase of risk identification that is carried out in risk assessment (see Figure 4.2).

Returning to the simple illustrative SoS introduced earlier (refer Figure 4.3), we consider three disruptions: (a) disruption of the bus, (b) disruption of the ferry, and (c) disruption of the subway train. This set is described by eq. (1).

$$Set\ of\ potential\ disruptions = \{(Bus), (Ferry), (Subway)\} \quad (1)$$

Note that it is possible for multiple vehicles to be disrupted simultaneously. However, for the sake of simplicity and to highlight the results of each phase in the resilience design process we only consider single-system disruptions in this example.
In the next phase, we determine how each of these disruptions impacts the SoS.

4.3 Estimate Impacts of Disruptions (Phase 2)

To develop the system importance measures we begin by considering the desired SoS performance, meaning, in the absence of any disruption, how should the SoS function/operate? Figure 4.8 shows the **desired (nominal) curve**. From a design perspective, this figure illustrates the desired performance level ($P_{Nominal}$) that the SoS is designed to maintain while in operation. The performance level and operational timeframe are specific to each SoS. For example, returning to the illustrative urban transportation SoS, typical measures of performance include passenger ridership, frequency of service, and average delay across the network. The operational lifetime of transportation networks is usually on the order of decades.

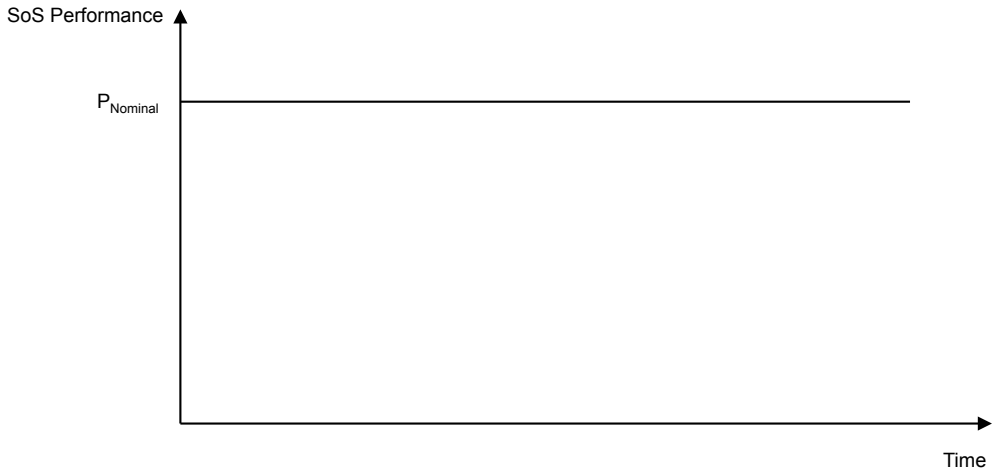

Figure 4.8 Example of a desired (nominal) curve

In practice, $P_{Nominal}$ in the desired curve may experience minor fluctuations as shown in Figure 4.9. For instance, airports regularly experience changes in traffic flow due to the prevailing winds. In such cases, we use the mean value across these fluctuations to determine a suitable $P_{Nominal}$ level.

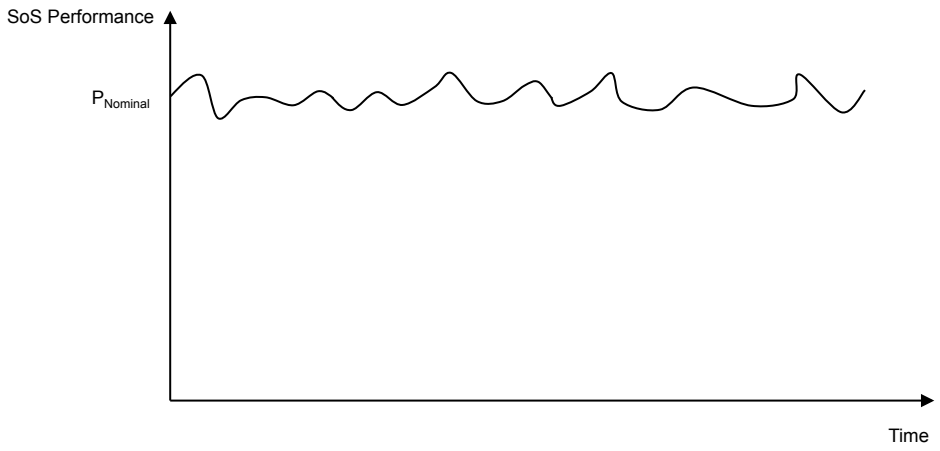

Figure 4.9 Illustration of variability in $\boldsymbol{P_{Nominal}}$

Next we investigate the impact of a particular disruption on the SoS. Figure 4.10 represents the **disruption curve**. When some disruption occurs, one or more systems in the SoS are affected. In this figure we assume that a single system (System *i*) is disrupted at $T_{initial}$, leading to a subsequent drop in the SoS performance level from the desired value ($P_{Nominal}$) to a lower value (P_{Loss}). The value stays low till the disrupted system is repaired or replaced at T_{final} when the SoS performance level is returned to $P_{Nominal}$. For example, in an urban transportation SoS, unscheduled subway line repairs can reduce throughput and cause delays on the rail mode, resulting in a reduction in the overall performance of the urban transportation network. However, some residual performance remains as existing road (buses and trams) and water (ferry) transportation modes continue to provide service to/and from neighboring cities. Note that at this stage of the resilience analysis, mitigation strategies, such as running extra subway trips or re-routing buses to compensate for the performance loss, are not considered. The original nominal performance level is restored when the repairs are complete and the subway system is completely operational again. While in Figure 4.10 only one system, System *i*, is disrupted, a similar curve can be used to depict the impact of a multi-system disruption.

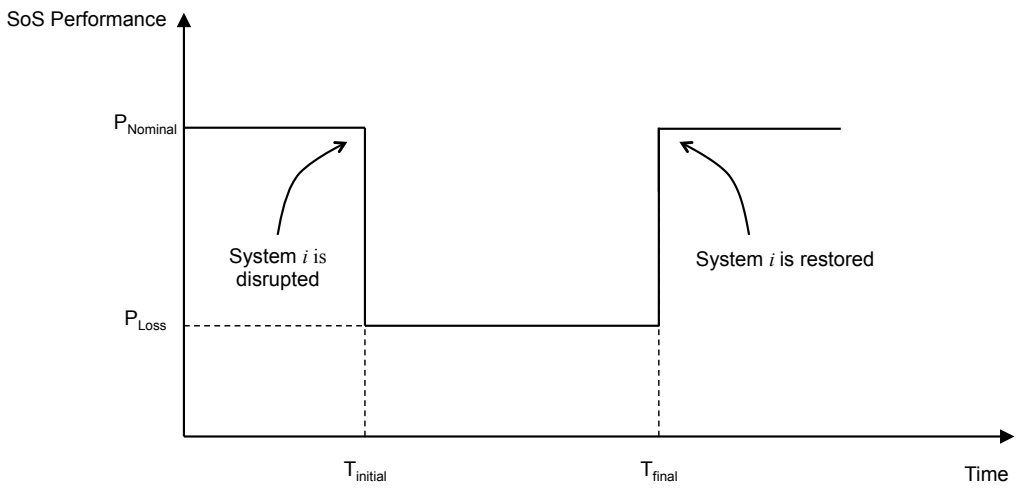

Figure 4.10 Example of a disruption curve with System *i* disrupted and System *i* restored without mitigation actions

Note that in the aftermath of a disruption, SoSs do not necessarily experience a sharp drop in performance or even a sharp increase in performance once the disrupted system has been restored as depicted in Figure 4.10. In many cases, gradual decreases and increases (see Figure 4.11) are observed. For example, consider the closure of an airport due to a snowstorm. As the storm abates, some runways are typically cleared sooner than others allowing partial performance increases as the entire airport is "restored" gradually. A similar curve can be used to represent multi-system disruptions where multiple systems are disrupted and restoration of all the disrupted system results in a return to $P_{Nominal}$ (see Figure 4.12).

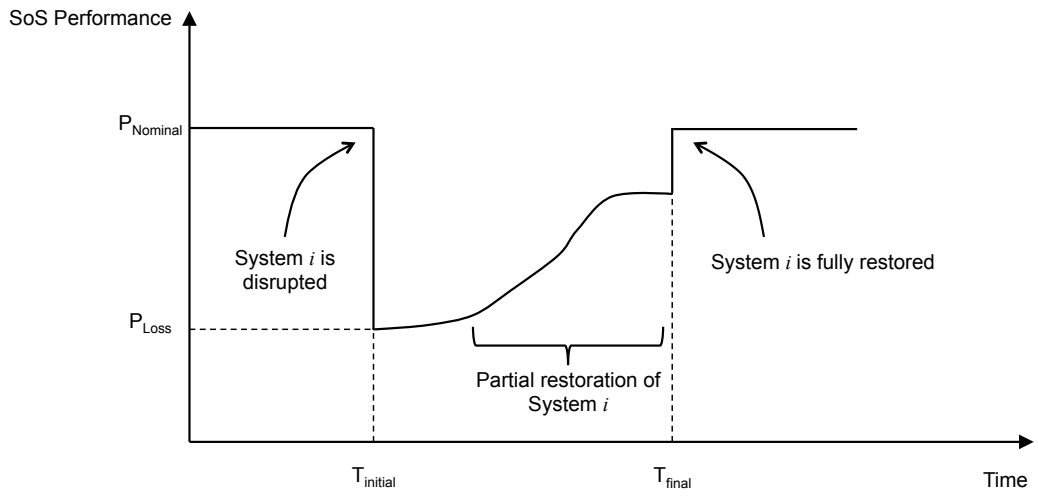

Figure 4.11 Disruption curve with gradual restoration of the disrupted system

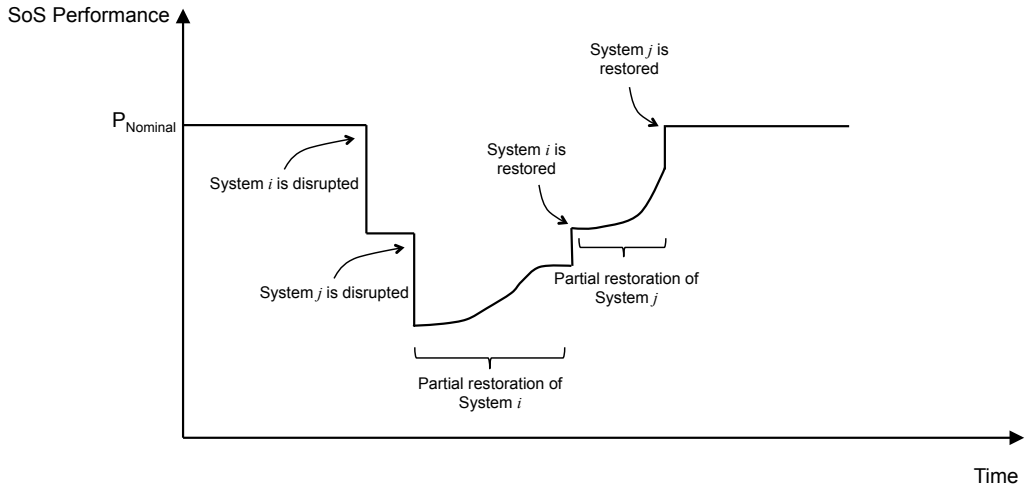

Figure 4.12 Example of a disruption curve for a multi-system disruption: System i disrupted followed by System j disrupted, and System i restored followed by System j restored

Also, Figure 4.10 indicates that in the absence of any mitigation measures, SoS performance is restored to its nominal level when the original "disrupted" system is restored (for example, by repairing or replacing it). Note that this may not always be the case. In some instances, for example in time-constrained military missions, failed systems are not repaired or replaced within the mission's time frame. Instead, the mission

continues with the available resources. In Chapter 5 we further discuss the application of the resilience design framework to such military missions through the use of a case study.

Against this backdrop, we now present the first importance measure, **System Disruption Importance**.

4.3.1 System Disruption Importance

The System Disruption Importance captures the impact of unmitigated disruptions. To develop this measure, we follow two steps. First, we determine **how much** a disruption (from the set identified in Phase 1) affects the overall SoS, and second, we determine **how important** this effect is relative to other disruptions. Redrawing Figure 4.10, we observe that the hatched region in Figure 4.13 represents the impact of an unmitigated disruption on the overall SoS. This impact, termed $Impact_D$, can be calculated using:

$$Impact_D = \int_{T_{initial}}^{T_{final}} f(t) - h_D(t) \qquad (2)$$

Here the subscript *D* refers to a disruption from the set identified in Phase 1.

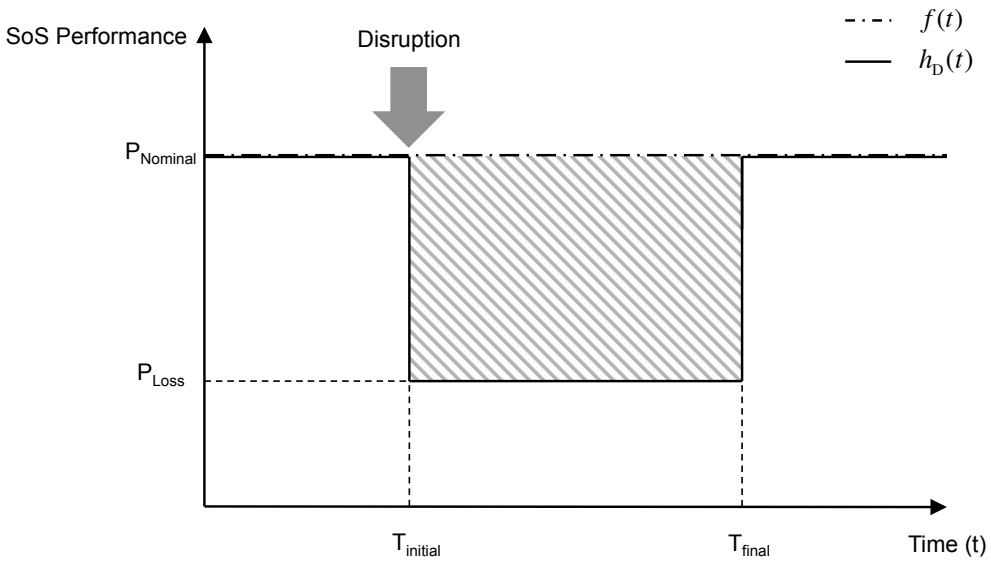

Figure 4.13 Disruption curve with $Impact_D$ highlighted (hatched region)

The System Disruption Importance (SDI_D) determines the relative importance of an unmitigated disruption, and is calculated using eq. (3):

$$SDI_D = \frac{Impact_D}{Worst\text{-}case\ SoS\ impact} \tag{3}$$

Again, here the subscript *D* refers a disruption from the set identified in Phase 1.

The denominator in the above equation is a measure of the worst-case impact on the SoS. This value is domain and SoS specific and can be estimated using, among others, historical data (e.g.: when studying the National Airspace SoS, closure of the US airspace in the three days following the 9/11 attacks can be a measure of the worst-case disruption impact) or simulation tools (as will be demonstrated in Chapter 5). SDI_D provides an indication of the relative importance of different unmitigated disruptions. For instance, those disruptions with large SDI_D values, i.e., those with large hatched regions, have the greatest impact on the SoS when they occur (since no mitigation measures, other than restoring the affected systems are considered). Thus, based on the SDI_D values, a ranking can be obtained of the relative importance of different disruptions. Note that the worst-

case value (denominator in eq. (3)) can be changed or updated without affecting the importance of different disruptions since all SDI_D are normalized using the same worst-case value.

Partial disruptions are also possible. For example, a landing gear malfunction may require an entire runway to be sprayed with foam for an emergency aircraft landing. Depending on the airport, such a situation can disrupt services on one runway for several hours while other runways are still in operation. Thus, the airport functions at a performance level between its nominal and full disruption (e.g. blizzard) values (see Figure 4.14).

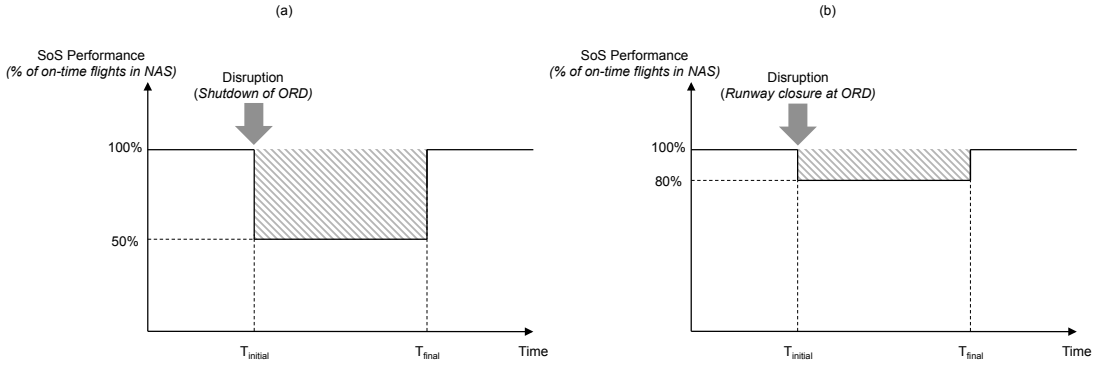

Figure 4.14 Notional example of full and partial disruptions: (a) impact of complete shutdown of ORD on National Air Space (NAS) and (b) impact of a runway closure at ORD on NAS

4.3.2 Outcome of Phase 2

The outcome of Phase 2 is a list (**ranking**) of the impacts of different unmitigated disruptions. We demonstrate the process of ranking the disruptions by returning to the simple illustrative SoS (refer to Figure 4.3). The disruption curves as well as $Impact_D$ values for the disruptions identified in Phase 1 are shown in Figure 4.15.

Assuming a worst-case SoS impact of 110 units, we can compute SDI_D for all three disruptions using eq. (3), as shown in Table 4.3. From these values, the relative importance of the different disruptions can be captured (third column of Table 4.3): a low ranking (e.g.: Ferry disruption) indicates a relatively low impact on SoS performance, while a high ranking (e.g. Subway disruption) indicates a disruption that has a large impact on the SoS.

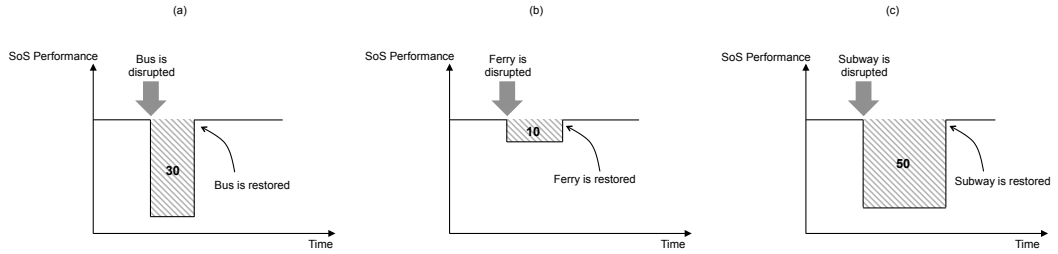

Figure 4.15 Disruption curves for illustrative SoS example (numbers in bold indicate $Impact_D$ values)

Table 4.3 $\boldsymbol{SDI_D}$ and importance ranking for illustrative example

Disruption (D)	**System Disruption Importance (SDI_D)**	**Importance ranking**
Bus	$SDI_{Bus} = 0.27$	2
Ferry	$SDI_{Ferry} = 0.09$	3
Subway	$SDI_{Subway} = 0.45$	1

4.4 Determine Current SoS Resilience (Phase 3)

In Phase 3, we consider mitigation measures. System-of-systems typically have some recovery strategies and contingency plans in place to handle disruptions. The **resilience curve** in Figure 4.16 provides an example of one mitigation measure: the ability of a system, here System *j*, to provide partial recovery when one or more systems in the SoS are disrupted. Given the availability of the mitigation measure that can be deployed at time $T_{mitigation}$, the SoS performance can be raised above P_{Loss} to some intermediate level ($P_{Mitigated}$) till the original system(s) that provided the capability is (are) restored.

For example, consider an urban transportation SoS. Unscheduled line repairs on subway tracks can reduce throughput and cause delays, resulting in a reduction in the overall performance of the urban transportation network. However, additional bus service between stations on the affected rail line can compensate for some of this lost performance.

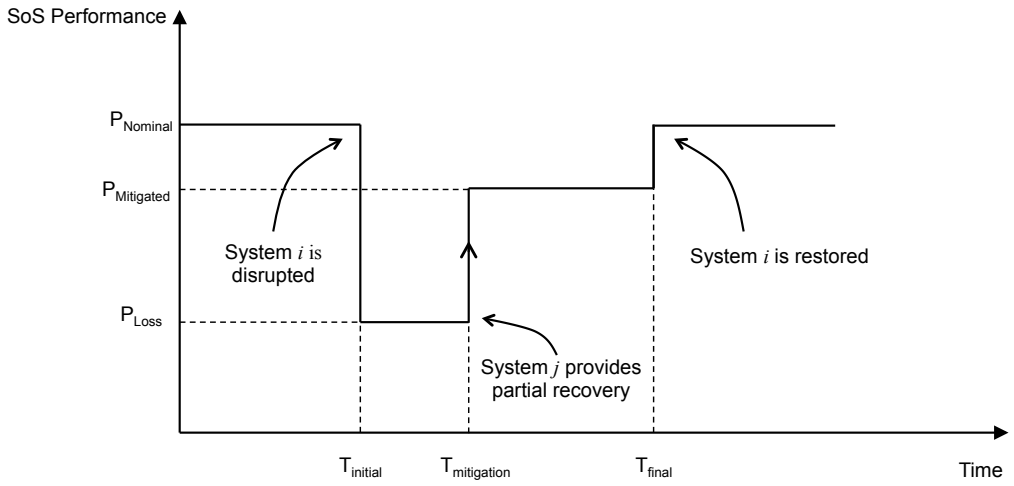

Figure 4.16 Example of a resilience curve

The mitigation path can take many different forms, depending on a variety of factors, including SoS topology and the specific system(s) used in the recovery. For example, the resilience curve may follow a linear path (as shown by the dashed line in Figure 4.17), a step path (dotted line), or perhaps even a recovery path that provides increased performance for a short duration before returning to the nominal SoS performance level (dashed-dotted line).

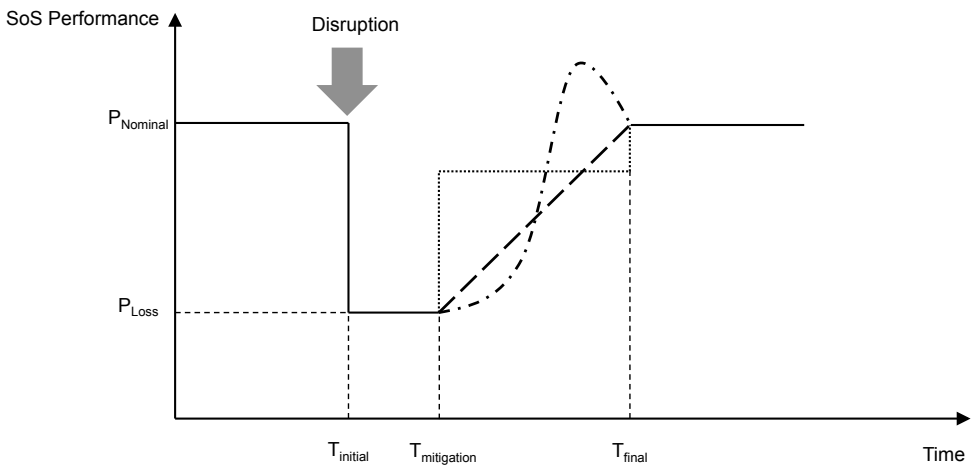

Figure 4.17 Notional resilience curves indicating different mitigation strategies

In this phase of the design approach, we evaluate the current SoS resilience and highlight key areas where improvements are needed or where downgrades can be made. To achieve this goal, we present the next two importance measures, **System Disruption Conditional Importance** and **System Disruption Mitigation Importance**.

4.4.1 System Disruption Conditional Importance

Referring to the hatched area in Figure 4.18, the System Disruption Conditional Importance ($SDCI_{D,M}$) is calculated using eq. (4) and answers the question: what is the relative importance of a mitigated disruption?

$$SDCI_{D,M} = \frac{\int_{T_{recovery}}^{T_{final}} f(t) - g_{D,M}(t)}{Worst\text{-}case\ SoS\ impact} \tag{4}$$

Here, as before, the subscript *D* refers to a disruption from the set identified in Phase 1, and the subscript *M* refers to a mitigation measure that can provide partial recovery of SoS performance when *D* occurs.

There are several ways to mitigate disruptive impacts. For instance, in the aftermath of a disruption (e.g.: flooding of a subway tunnel), a single system (e.g., one bus) or multiple systems (e.g., multiple buses and/or increased car pooling) can be used to provide partial recovery till the subway is restored. When considering multi-system mitigations, given the domain-specific structure and behavior of SoSs, curves for combined recovery are not necessarily linear combinations of the individual system recoveries. Typically, SoS engineers would use suitable simulations and models to assess the mitigation effectiveness of multi-system recovery (further discussed in Chapter 5).

Observe that since mitigations reduce the impact of disruptions, the hatched area in Figure 4.18 is smaller than in the previous case (Figure 4.13). Specifically, a low $SDCI_{D,M}$ shows that the impact of the disruption has been mitigated, and vice versa. Note that when mitigation is not provided or designed $SDCI_{D,M}$ is undefined. We discuss in Section 4.4.3 how the analyst can determine what value of $SDCI_{D,M}$ constitutes an adequate mitigation.

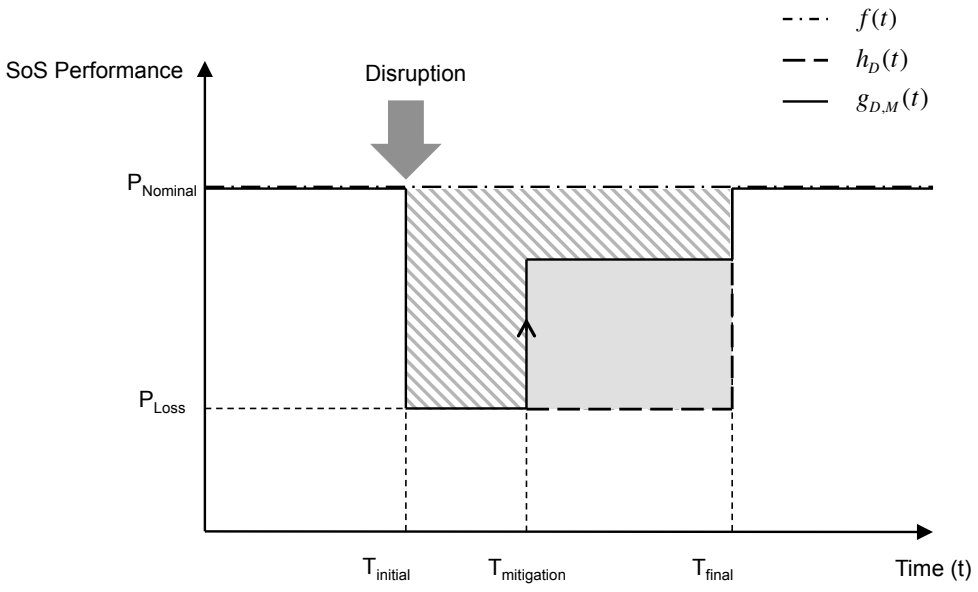

Figure 4.18 Resilience curve with $SDCI_{D,M}$ (hatched region) and $SDMI_{D,M}$ (solid grey region) highlighted

4.4.2 System Disruption Mitigation Importance

The second importance measure, System Disruption Mitigation Importance ($SDMI_{D,M}$), answers the question: what is the relative importance of the effectiveness of a mitigation measure in reducing the impact of a disruption? This measure is represented by the solid grey region in Figure 4.18 and is calculated using eq. (5):

$$SDMI_{D,M} = \frac{\int_{T_{recovery}}^{T_{final}} g_{D,M}(t) - h_D(t)}{Worst\text{-}case\ SoS\ impact} \tag{5}$$

Note that, similar to SDI_D and $SDCI_{D,M}$, $SDMI_{D,M}$ is also normalized by the earlier worst-case value and is undefined when mitigation is not possible. The larger the value of $SDMI_{D,M}$, the more important the mitigation measure is to reducing the impact of the corresponding disruption. Conversely, a low $SDMI_{D,M}$ indicates that the mitigation measure does not significantly alleviate the disruption impact.

In summary, SDI_D provides an assessment of the impact of unmitigated disruptions on the SoS while $SDCI_{D,M}$ and $SDMI_{D,M}$ evaluate effectiveness of mitigation measures in reducing these disruptive impacts (see Table 4.4).

Table 4.4 System Importance Measures

SIM	Question answered by SIM	Meaning	
		Low Value	High Value
System Disruption Importance ($\boldsymbol{SDI_D}$)	What is the relative importance of an unmitigated disruption	Disruption has low adverse impact on SoS	Disruption has high adverse impact on SoS
System Disruption Conditional Importance ($\boldsymbol{SDCI_{D,M}}$)	What is the relative importance of a mitigated disruption	Disruption, given its impact is mitigated, has low adverse effect on SoS	Disruption, given its impact is mitigated, has high adverse effect on SoS

SIM	Question answered by SIM	Meaning	
		Low Value	High Value
System Disruption Mitigation Importance ($\boldsymbol{SDMI_{D,M}}$)	What is the relative importance of the effectiveness of a mitigation measure?	Mitigation measure contributes little to SoS resilience	Mitigation measure has high contribution to SoS resilience

While overall mitigation effectiveness (as captured by $SDMI_{D,M}$) is important, in some instances the "quickness of recovery" (time to start of mitigation after a disruption) and the "level of recovery" (amount of SoS performance recovered by the mitigation) can be valued differently. There may also be cases where time or performance is non-linear. For example, if providing even poor alternative transportation modes during rush hour may be better than waiting for better modes. Chapter 6 discusses potential ways to address it in future work.

4.4.3 Outcome of Phase 3

The outcome of Phase 3 is two-fold: (1) a **ranking** of the impacts of different disruptions given the availability of mitigation measures, and (2) a **resilience map**. To explain the two outcomes, we return to the simple illustrative example described earlier (see Figure 4.3) . Let us now consider three mitigation strategies that the SoS, in its current configuration, employs (refer to Figure 4.19):

1. When the Bus is disrupted, a backup Bus is deployed, till the original bus is restored (see Figure 4.19(a)).
2. When the Ferry is disrupted, the Subway is able handle some of the spillover traffic as passengers can walk to the nearest subway station (see Figure 4.19(b)).
3. When the Subway is disrupted, the Bus and the Ferry partially compensate for the lost performance (see Figure 4.19(c)).

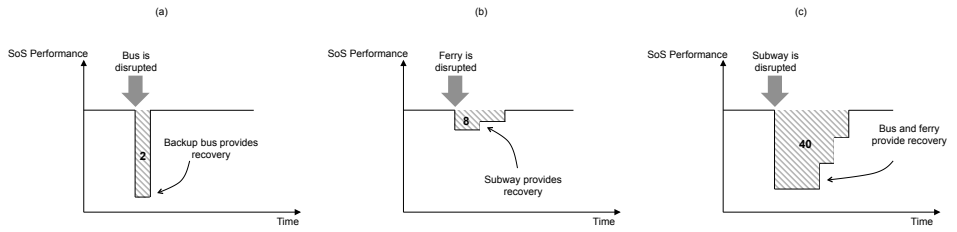

Figure 4.19 Resilience curves for illustrative SoS example (numbers in bold indicate areas for $SDCI_{D,M}$ calculation)

To build the resilience map we first consider the individual $SDCI_{D,M}$ values. The rows in Figure 4.20 indicate disruptions while the columns indicate mitigation measures. Where mitigation is possible, the corresponding cells are populated with $SDCI_{D,M}$ values calculated using eq. (4). Recall that, where mitigation is not possible, the cells are undefined. Averaging all potential mitigation options across each row provides the mean $SDCI_{D,M}$ for each disruption. This value is a measure of how well the mitigation measures have helped reduce disruptive impacts.

The new relative importance of the different systems can now be determined (third column of Table 4.5). Observe that with the mitigation strategies available in the current SoS, the Bus has a lower ranking than the Ferry than in the case without mitigation measures (refer to Table 4.3).

Set of Disruptions	Bus	Ferry	Subway	Backup bus	Bus and ferry	avg. $SDCI_{D,M}$
	Set of Mitigations					
Bus				0.02		0.02
Ferry			0.07			0.07
Subway					0.36	0.36

Figure 4.20 $SDCI_{D,M}$ for illustrative SoS example

Table 4.5 $SDCI_{D,M}$ and importance ranking for illustrative example

Disruption (D)	System Disruption Conditional Importance ($SDCI_{D,M}$)	Importance ranking
Bus	$SDCI_{Bus,Backup\ Bus} = 0.02$	3
Ferry	$SDCI_{Ferry,Subway} = 0.07$	2
Subway	$SDCI_{Subway,Bus+Ferry} = 0.36$	1

While we know the overall importance of the different disruptions, we now need to determine how resilience to these disruptions can be improved.

In reliability and risk analysis, practitioners frequently specify minimum acceptable performance levels to assess risk mitigation measures and safety training – if the performance of a system or subsystem falls below a pre-determined level, immediate steps must be taken to address this undesirable situation. These minimum acceptable levels depend on many factors such as regulatory standards, operator workload and training, system design, and public acceptance.

In a similar vein, here we introduce a decision threshold (α) to assess the importance of the different systems. The decision threshold is the maximum acceptable $SDCI_{D,M}$ and is used to generate the resilience map (see Figure 4.21). We describe how this threshold can be set in Chapter 5. In this example, assuming $\alpha = 0.1$ and comparing each $SDCI_{D,M}$ to this value of α each cell in the map is allocated a specific color as follows: red when $SDCI_{D,M} > \alpha$ and green when $SDCI_{D,M} < \alpha$. Darker shades of red indicate disruptions are highly unmitigated, while darker shades of green indicate disruptions that are currently handled well.

The resilience map summarizes the relevant resilience information in two ways: (1) high level overview of which disruptions have been mitigated adequately and which ones have

not, and (2) detailed information about which disruption-mitigation combinations need attention.

At the high-level, by comparing the first and last columns of the resilience map, we see which disruptions have been mitigated (when SDI_D value is red and the corresponding average $SDCI_{D,M}$ is green), and which ones have not (when SDI_D and average $SDCI_{D,M}$ are both red). The extent to which the strategies mitigate the disruptive impacts is proportional to the difference between these two values in each row. For ease of explanation we do not include a discussion of average $SDMI_{D,M}$ here (design implications of these values will described in Chapter 5).

Next, we study the resilience map in detail to determine potential design changes that can aid resilience improvement. Section 3.2.1 presented a set of ten design principles that can be used to drive changes in SoS architecture based on the particular needs of the particular SoS under study. As mentioned previously, the list is not exhaustive, and as researchers and practitioners determine new ways to improve SoS designs, this set can be modified and expanded. Focusing on specific disruption-mitigation pairs, the resilience map points to different types of improvement strategies. Here we highlight key suggestions for the illustrative example based on Figure 4.21 (Chapter 5 presents additional and more interesting design implications through case studies):

1. **Observation:** The red cell in the last row indicates that disruption of the Subway has not been adequately mitigated.
   Specific problem (a): Both the Bus and the Ferry do not have adequate capacity to handle the spillover demand.
   Potential solution: *Physical redundancy* can improve the capacity of the mitigation measures. One way to realize physical redundancy is to maintain spare ferries and buses, which can be called in to service when there is a Subway disruption.

Specific problem (b): High impact (low survivability) of the Subway disruption.
Potential solution: *Drift correction* can improve the survivability of the Subway. One way to realize drift correction is to maintain sensors in the subway tunnel to monitor water levels and thereby control water pumps automatically – this technique allows some subway lines to continue operating through minor floods.

Note: In a more general sense, the use of different colors to highlight nuances within SoS resilience is useful because it allows decision-makers to not only consider the most important systems (obtained from the earlier ranking process) but also visualize, in an intuitive way, specific areas of inadequate resilience within the SoS. Thus, the map enables decision-makers to consider multiple opportunities to improve SoS resilience, such as, for example, the ability to make minor improvements to several moderately important systems rather than focus only on the most important one.

2. **Observation:** While the backup Bus is clearly quite effective in mitigating the impact of a Bus disruption, it remains unused when the Subway is disrupted.
   Opportunity: We could potentially use the backup Bus more effectively by deploying it in the event of disruptions (e.g.: Subway disruptions) other than the one it is intended to address (e.g.: Bus disruption).

   Note: These types of observations from the resilience map help decision-makers move away from the stovepipe approach of considering each mode individually (e.g.: spare buses to be used when primary buses encounter mechanical failures) and instead identify resources that can be used across different modes.

3. **Observation:** Cells shaded grey indicate those that mitigations that do not currently contribute to SoS resilience. For instance, when the Ferry is disrupted, the Bus does not provide mitigation.

Suggested improvement: The resilience map highlights the lack of mitigation for particular disruptions. If the SDIs corresponding to the grey cells are sufficiently low (first column of the map), the grey cells can be left as is (in other words, although the disruption is not mitigated, it is small and does not require mitigation). However, if the SDI and $SDCI$ is high, the SDI should be lowered by reducing the impact of the unmitigated disruption, or the $SDCI$ should be lowered by adding mitigations. Potential mitigations can be identified by considering the columns in the map. For instance, by providing shuttle service for passengers from the Ferry landing to the Bus depot, we can leverage the Bus to mitigate a Ferry disruption.

Note: While this suggestion may seem obvious, the true value of this recommendation is realized when the resilience framework is used to study larger networks (as will be highlighted in Chapter 5). For these SoSs, the visual nature of the resilience map provides a useful way to summarize those disruptions that remain unmitigated and those mitigation strategies that do not contribute to resilience.

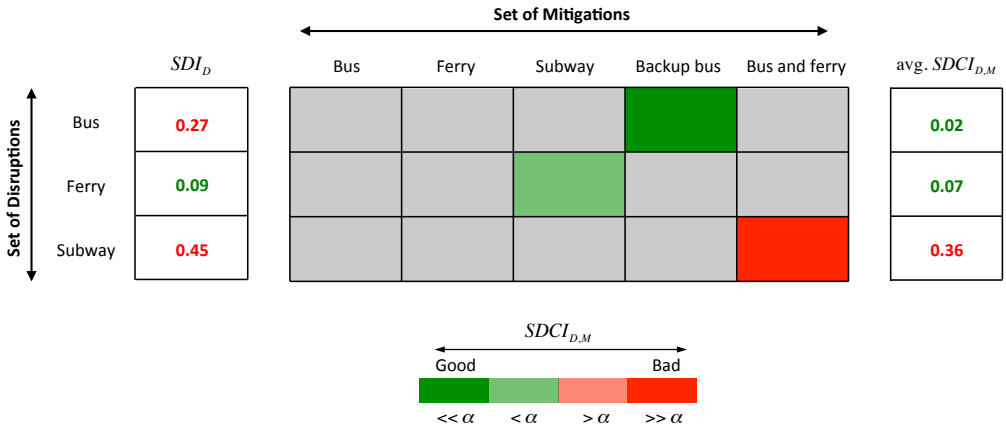

Figure 4.21 Resilience Map for $\alpha = 0.1$

The value of α can range between 0 and 1, where 0 indicates the the SoS is disruption proof while 1 indicates that the SoS is un-resilient. Determining a suitable α depends on

multiple factors such as the particular SoS under investigation, available resources, cost of the mitigation measures, and the decision-maker's judgment. Additionally, in practice, due to the same factors, the value of α may need to be varied during the decision-making process. Thus, here, we propose an iterative approach to determining an appropriate α value (discussed further in Chapter 5 through the use of case studies). Potential ways to determine an initial value include considering the minimum acceptable performance level for an SoS (e.g.: average delay in a transportation network should not exceed 45 min), historical data (e.g.: delays experienced in the National Air Space during previous disruptions such as snowstorms and hurricanes), and expert opinion.

Varying α changes the resilience map. While the overall SIM values do not change, the color of each cell changes as α varies. For instance, Figure 4.22 and Figure 4.23 show how the resilience map for the illustrative example changes for $\alpha = 0.4$ and $\alpha = 0.05$ respectively. Observe that for the higher α value (risk-taking analyst), all the cells are some shade of green, indicating that no "areas of concern" exist. In contrast, for the lower α value (risk averse analyst), some cells that were previously colored green have now turned red. So, in terms of practical usefulness, an analyst can study how colors on the resilience map change as the value of alpha "slides" between high and low values. By identifying the cells that remain red across a range of alpha values, the analyst can determine mitigation strategies that need to be improved (prioritize resource allocation) or studied in further detail (guidance for simulations and field tests).

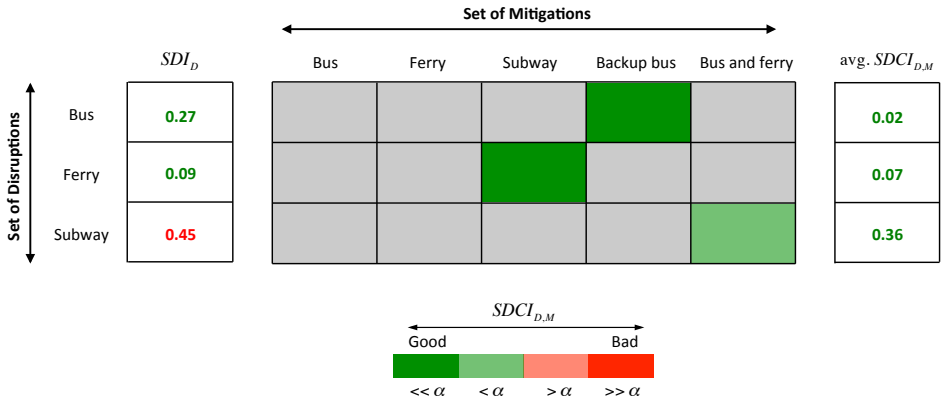

Figure 4.22 Resilience Map for $\alpha = 0.4$

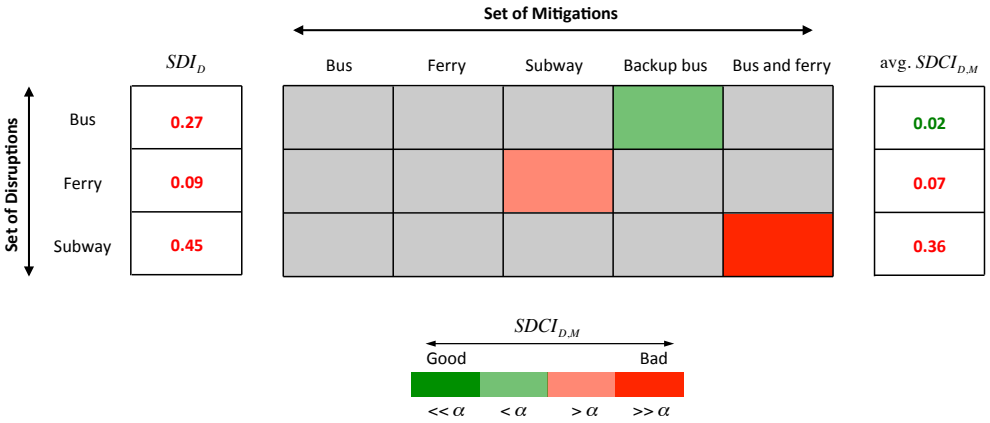

Figure 4.23 Resilience Map for $\alpha = 0.05$

4.5 Improve SoS Resilience (Phase 4)

In Phase 4 of the resilience framework, the potential design improvements suggested in Phase 3 are implemented and the SIM analysis is conducted again. The updated resilience map indicates whether (or not) the design changes have yielded the desired results. The obvious next step in a design process is the evaluation of suitable design changes. While conducting a suitable analysis of alternatives is beyond the scope of this thesis, this step will be part of future work of this research. To conduct a comprehensive analysis of alternatives, several factors must be considered. For example, some questions that should be part of any qualitative or quantitative analysis include:

- How much does the design change cost?
- How effective is the design change?
- How easy is it to implement the change?
- Does the change have unintended consequences? (e.g.: new common cause disruptions, new training/human factors issues)

4.5.1 Outcome of Phase 4

The outcomes of Phase 4 are similar to those of Phase 3, that is (1) a **ranking** of the impacts of different disruptions given the availability of mitigation measures, and (2) a **resilience map**. Once the design improvements are made and the SoS is re-analyzed, the system importance ranking and the resilience map are updated to reflect the changes. If the design modifications are inadequate or impractical (e.g. too expensive, hard to implement, organizational hurdles), new design principles can be considered and once again, the resilience map is updated.

Returning to the simple SoS example, Figure 4.21 pointed to inadequate mitigation of the disruption of the Subway by the combined capabilities of the Bus and the Ferry, and suggested using the principle of drift correction to improve the design. The updated resilience map in Figure 4.24 reflects this design improvement (see green cell in the last row).

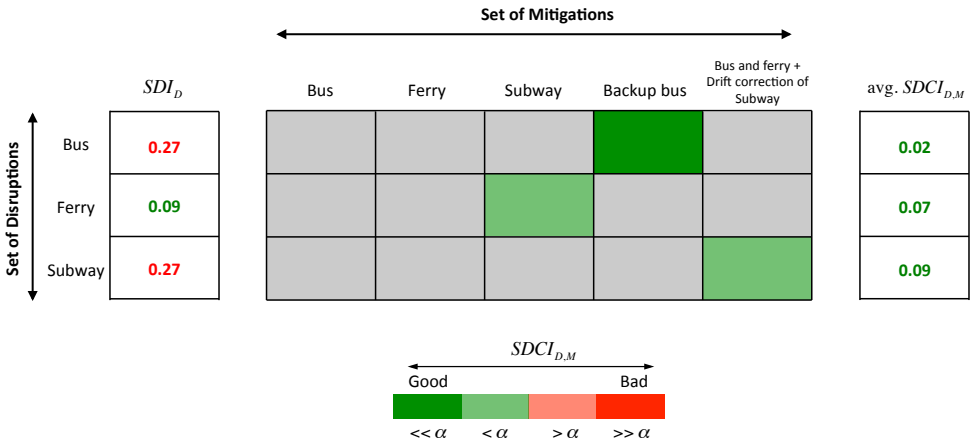

Figure 4.24 Updated Resilience Map (for $\alpha = 0.1$)

4.6 Summary

As described in Section 1.2, the characteristics of systems-of-systems make analysis and design of resilience challenging. However, these features also offer opportunities to make SoSs resilient using unconventional methods. In this chapter, we adapted the traditional risk-based design process to include two SoS-focused features. First, system importance measures (SIMs) determine the relative importance of different systems based on their impacts on SoS-level performance. Second, suggestions for resilience improvement draw from design options that leverage SoS-specific characteristics, such as the ability to adapt quickly (such as add new systems or re-task existing ones) and to provide partial recovery of performance in the aftermath of a disruption.

The four phases of the design process can be used to study the resilience of both existing (fielded) SoSs and new (un-deployed) SoSs. In the case of the former, the resilience map highlights how well or how badly the current SoS structure can handle disruptions and points to inadequacies that need to be addressed. For the latter type of SoS, resilience map helps evaluate the resilience of potential SoS architectures.

Specific advantages of the SIM-based resilience design include:

- **Allows rapid understanding of different areas of concern within the SoS.** The visual nature of the resilience map (a key outcome of the SIM analysis) provides a

useful way to summarize the current resilience of the SoS as well as point to key systems of concern.

- **Provides a structured approach to resilience management.** Using the design framework, decision-makers are guided through the analysis of SoS resilience in a systematic way, starting from the identification of disruptions to iterating in a group setting to improve SoS resilience.
- Provides a platform for multiple analysts and decision-makers to **study, modify, discuss and document** options for SoS.

In the next chapter, we demonstrate the applicability of the resilience framework to real-world SoSs through the use of two case studies.

CHAPTER 5. APPLICATION OF SIM-BASED RESILIENCE DESIGN: DEMONSTRATION STUDIES

In this chapter, we use two case studies to demonstrate how the SIM-based design framework can be used to inform decision-making in the context of SoS resilience.
The first case study is a naval warfare SoS and illustrates the application of SIMs to military missions, while the second case study focuses on an urban transportation SoS. The two SoSs have different objectives and different characteristics. These features enable us to show how the SIM-based approach is applicable to different types of SoSs and to highlight major aspects and results of the design process. For instance, while the primary focus of the urban transportation SoS is the efficient movement of people, the objectives of time-sensitive military missions can vary widely, such as search-and-rescue, surveillance, or target elimination. Also, transportation SoSs typically have longer operational lifetimes, with new systems being interfaced with legacy systems, than combat SoSs. Consequently, both SoSs face different types of disruptions. As will be discussed in this chapter, the abovementioned characteristics have implications for defining SoS performance and determining how the various design principles can be implemented to improve resilience.

We use each case study to draw attention to different aspects of the resilience framework. In the naval warfare case study, we describe how the resilience framework can leverage existing simulation models to support end-to-end design. We proceed through the four phases of the approach using an agent-based model (ABM) that enables us to demonstrate how simulation tools and analytical models can be used to determine the necessary inputs for the framework and subsequently, to inform decision-making regarding SoS resilience

The urban transportation case study in contrast focuses on interpreting the results of the resilience framework and on describing how they can be used to guide design choices in large infrastructure networks. We use different resilience maps to highlight the range of design-related information that can be obtained from the framework

5.1 Case Study 1: Naval Warfare SoS

The mission of the naval warfare system-of-systems studied here is to conduct near-shore search-and-destroy operations, similar to those carried out by the Coast Guard and littoral combat units in the Navy. Figure 5.1 illustrates the area of interest and the systems in the SoS. The specific task of the SoS is to find and destroy the enemy boat within the planned mission time (PMT) of 4 hours. There are four systems in the SoS that collaborate to achieve the overall objective: a Ship, a Helicopter, an Unmanned Aerial Vehicle (UAV), and a Satellite. The capabilities of each system and the communication links between them are described in Table 5.1.

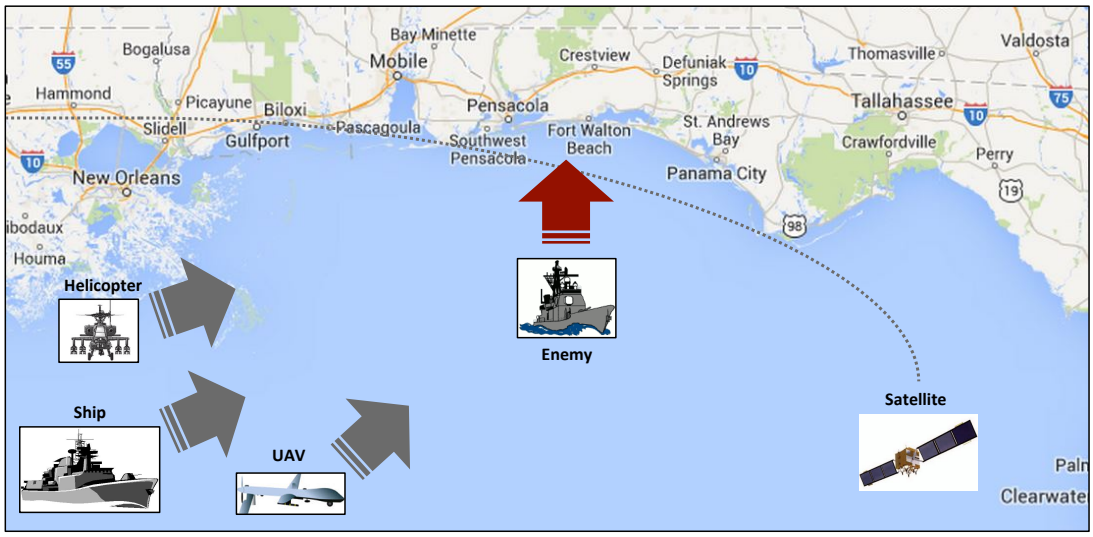

Figure 5.1 Naval warfare SoS

Table 5.1 Systems in naval warfare SoS

System	Capabilities	Communication links
Ship	Detect enemy (radar) Eliminate enemy (weapons)	Send to and receive information from Helicopter and UAV Receive information from Satellite
Helicopter	Detect enemy (radar) Eliminate enemy (weapons)	Send to and receive information from Ship
UAV	Detect enemy	Send to and receive information from Ship
Satellite	Detect enemy	Send information to Ship

We use an agent-based model (ABM) (adapted from Mour et al. [2013]) to simulate and study the naval warfare SoS. Parameters such as weapons range, velocity, fuel tank capacities, and radar detection ranges for each agent can be varied to simulate different recovery options. In the following sections, we proceed through the four phases of the SIM-based approach and illustrate how the proposed framework facilitates decision-making in the context of the naval warfare SoS.

5.1.1 Phase 1: Identify Potential Disruptions

Military missions can encounter many types of disruptions. For example, systems may be disrupted by enemy attacks, internal subsystem failures, or even adverse weather. Partial disruptions are also possible, such as, for instance, a disruption of intra-SoS communications due to electronic jamming.

In this case study, we investigate three types of disruptions: single system disruptions (due to targeted enemy attacks or random failures), multi-system disruptions (due to common cause failures and/or cascading failures), and partial disruptions (see Figure 5.2). In total fourteen disruptions are studied (11 full disruptions and 3 partial disruptions).

Since only the Ship and Helicopter carry weapons and given that mission success depends on the ability to eliminate the enemy boat, any disruption that has both these systems failing is not considered in this study. In these cases, we assume that the mission

is aborted. Additionally, we consider partial disruptions of the Ship and Helicopter. The Ship has two important functions in the mission: (1) collect, integrate, and distribute information to the other systems and (2) eliminate the enemy boat using weapons. Hence, we consider two partial disruptions of the Ship: (1) failure of the communications subsystem on the ship rendering it unable to co-ordinate with the other systems and, (2) inability of the Ship to launch its weapons. Similarly, partial disruption of the Helicopter is a weapons failure.

Given these example disruptions, the agent-based model can demonstrate how well the SoS performs in the face of these disturbances (described in Phase 2). If however, the aim were to study the overall effect of a range of disruptions, then we would need to consider the probabilities that these disruptions occur. Chapter 6 discusses ways to incorporate uncertainties into the SIM analysis.

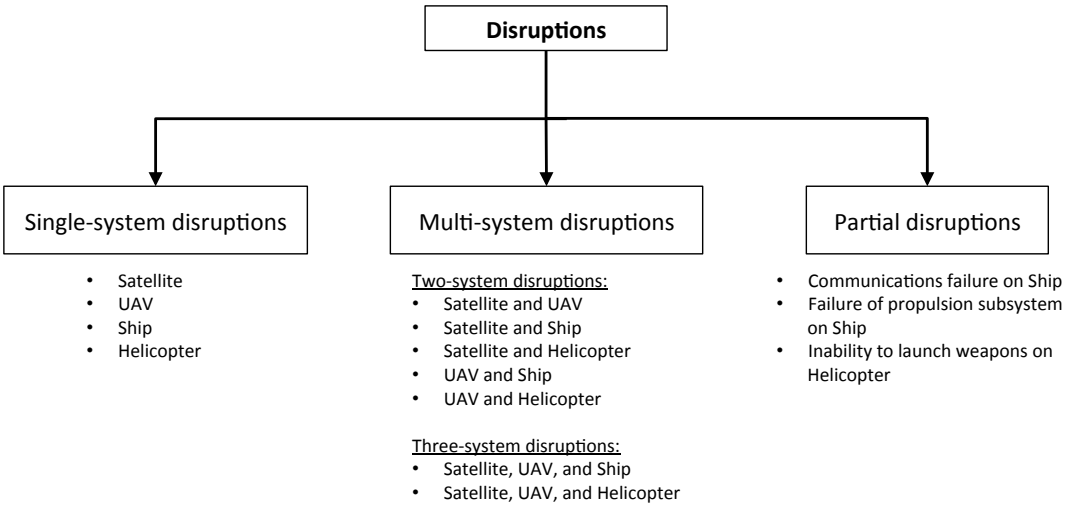

Figure 5.2 Potential disruptions in naval warfare SoS

5.1.2 Phase 2: Estimate Impacts of Disruptions

When assessing the performance of military missions, primary parameters of interest are:

1. Mission success: Will the mission be successful in carrying out its objectives within the planned mission time?
2. Mission completion time: How soon can the mission be completed?

In this study, to illustrate the application and outcomes of the design process, we focus on **mission success** (elimination of the enemy boat within the planned mission time) as a measure of the SoS performance.

To account for uncertainty and randomness in agent behavior, a Monte Carlo analysis was conducted 1000 times for each SoS instance (e.g. SoS with no disruptions, SoS with disrupted UAV, SoS with disrupted UAV and Ship, etc.). Subsequently, the mission success was calculated as shown below:

$$Mission\ success = \frac{No.of\ successful\ missions}{1000} \tag{6}$$

To establish nominal SoS performance, we ran the ABM without any disruptions and recorded the resulting mission success (94%).

Next, we determined the impact of the various disruptions identified in Phase 1. For time critical missions, the time at which a disruption occurs can have a significant impact on the performance. For instance, a disruption to the satellite late in the mission would have limited impact if the satellite had already detected the enemy and relayed the relevant information to other systems before being disrupted. Here, we looked at the potential disruptions and evaluated their impacts when they happen relatively early in the mission (at 1 hour) or late in the mission (at 2.5 hours). Table 5.2 summarizes the results. On average, and as expected, when disruptions happen early, they have a greater impact on the SoS performance than when they occur late in the mission. Exceptions are when either the Helicopter or communications on board the Ship are disrupted at 2.5 hours. Hence, through the rest of this chapter, we consider only early disruptions.

In this phase of the analysis, we assume that, in the event of a disruption, the remaining systems continue with the mission and that the disrupted system(s) return to base, that is, failed systems cannot be repaired or restored within the planned mission time.

Table 5.2 Impact of disruptions on mission success rates (naval warfare SoS)

Type of disruptions	**Disruption (*D*)**	**Mission Success Rate (%)**	
		Early disruption (at 1 hour)	**Late disruption (at 2.5 hours)**
Single system disruptions	Satellite	27	94
	UAV	93	94
	Helicopter	3	2
	Ship	0	92
Two-system disruptions	Satellite and UAV	1	94
	Satellite and Helicopter	0	4
	Satellite and Ship	0	93
	UAV and Ship	0	94
	Helicopter and UAV	0	2
Three-system disruptions	Satellite, UAV, and Helicopter	0	1
	Satellite, UAV, and Ship	0	93
Partial disruptions	Communications subsystem on Ship	1	4
	Propulsion subsystem on Ship	92	90
	Failure to fire weapons on Helicopter	9	9

From Table 5.2, it is clear that in the worst case, the mission success falls to zero. We now use this result to determine the worst-case SoS impact as follows: subtract the worst-case mission success rate (0%) from the nominal SoS performance (94%), and then multiply the resulting number by the duration of the disruption (4 hours, since in the worst case the disruptions can occur at the start of the mission). The process is shown in eq. (7).

$$\textit{Worst-case SoS impact} = (94 - 0) \cdot 4 = 376\ \textit{units} \qquad (7)$$

Next, the $Impact_D$ and SDI_D of each disruption are determined using eqs. (2) and (3). Table 5.3 presents the fourteen disruptions sorted in order from most to least important based on their SDI_i values. Some interesting observations include:

- Eleven unmitigated disruptions have fairly severe effects ($SDI_D > 0.6$) on the mission when they occur. Most of these disruptions include either the Ship or the Helicopter (fairly obvious since these are the only two systems that can carry weapons.
- The two types of partial disruptions of the ship have dramatically different impacts on the SoS. When the propulsion subsystem fails, rendering the ship immobile but still able to communicate with the other agents, the mission is not jeopardized ($SDI_D = 0.02$). However, a communications failure ($SDI_D = 0.75$) can stymie the mission even if the ship can proceed towards the enemy. This result is intuitive since the SoS configuration (see Table 5.1) shows that the ship is the central communications hub, and any failure of its communications capabilities implies that important tracking information does not get delivered to the other systems.
- Disruption of the UAV alone has little impact on the SoS mission. However, when both the UAV and the Satellite are disrupted, the combined impact on the SoS is larger than their individual impacts. Clearly, while the UAV alone may be redundant in the un-disrupted SoS, it contributes to surveillance when the Satellite is disrupted.

Table 5.3 SDI_D for naval warfare SoS

Disruption (D)	**SDI_D**	**Importance Ranking**
Ship	0.75	1
Satellite and Ship	0.75	1
UAV and Ship	0.75	1
Satellite and Helicopter	0.75	1
Helicopter and UAV	0.75	1
Satellite, UAV, and Helicopter	0.75	1

Disruption (*D*)	**SDI_D**	**Importance Ranking**
Satellite, UAV, and Ship	0.75	1
Communications subsystem on Ship	0.75	1
Satellite and UAV	0.74	9
Helicopter	0.71	10
Failure to fire weapons on Helicopter	0.68	11
Satellite	0.54	12
Propulsion subsystem on Ship	0.02	13
UAV	0.01	14

5.1.3 Phase 3: Determine Current SoS Resilience

While military personnel will have access to information regarding mitigation measures (recovery features, contingency plans, operating procedures) of military missions, we assume that the baseline SoS has three mitigations available to deal with disruptions:

1. The Ship is armed with additional higher-range weapons to compensate for an Helicopter disruption.
2. The UAV is equipped with a more powerful secondary radar (Mode 2 radar) to provide wide-area search capability when the Satellite is disrupted. This measure results in a heavier UAV that requires frequent returns to the Ship for refueling.
3. If the UAV is disrupted, it can be repaired within a certain time frame, here 1.5 hours after the disruption. The UAV would need to return to the Ship for inspection, repair, and re-deployment.

Again, we used the agent-based model to implement the above mitigations and evaluate their effectiveness. Next, we recorded the new mission successes to determine $SDCI_{D,M}$ values using eq. (4) (see Figure 5.3) and $SDMI_{D,M}$ values using eq. (5) (see Figure 5.4). The rows in both figures indicate disruptions while the columns represent mitigation strategies. Where mitigation is possible, the corresponding cells are populated with the calculated $SDCI_{D,M}$ and $SDMI_{D,M}$ values.

Now, we define a decision threshold (α) and use these $SDCI_{D,M}$ and $SDMI_{D,M}$ results to build the resilience map.

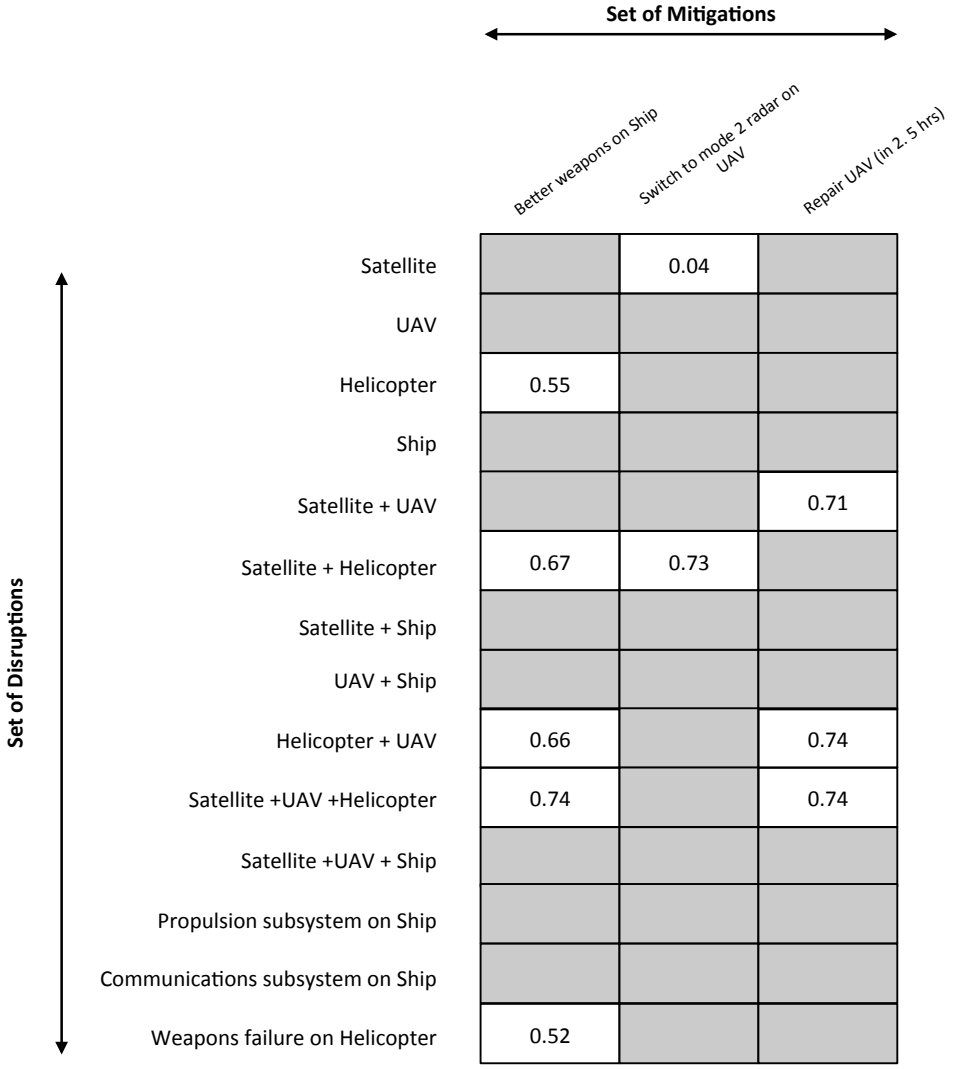

Figure 5.3 $\mathrm{SDCI_{D,M}}$ (Phase 3) for naval warfare SoS

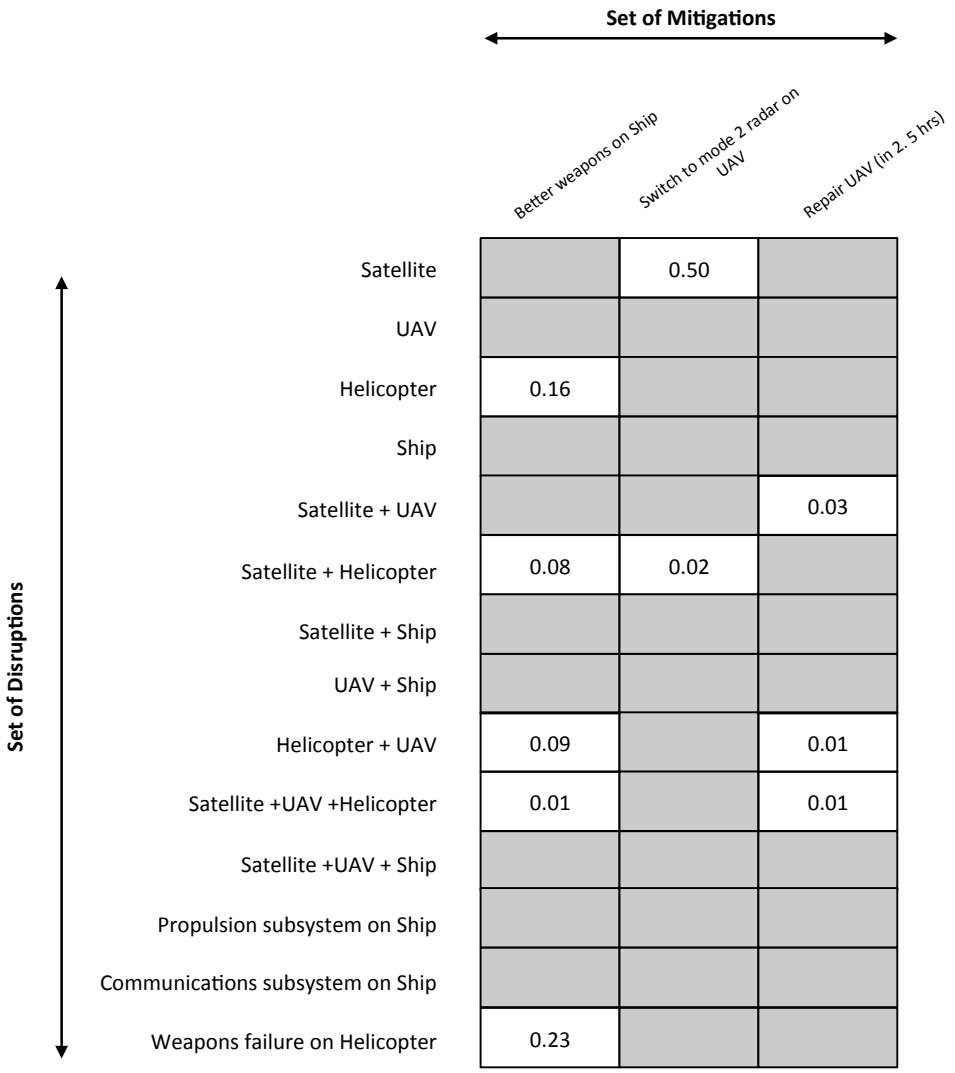

Figure 5.4 $\mathrm{SDMI}_{\mathrm{D,M}}$ (Phase 3) for naval warfare SoS

To determine an initial decision threshold we first establish a minimum acceptable mission success level. In practice, such a limit can be reached through analysis and consensus across a range of stakeholders such as among others commanding officers and combat operations specialists. Here, we assume that the minimum acceptable mission success is 60% if one or more systems are disrupted early (one hour into the mission). Now, using eq. (4), we see that the $SDCI_{D,M}$ corresponding to this minimum acceptable mission success rate is 0.27. Thus, the initial α is set to 0.27.

Next, we develop the resilience map for the naval warfare SoS (see Figure 5.5). As before, the first column in the map represents impact of unmitigated disruptions (SDI_D), while the last column denotes the impacts of the same disruptions once they have been mitigated (average $SDCI_{D,M}$). The color of each cell in the resilience map is determined by comparing its $SDCI_{D,M}$ value with α. At first glance, we note that in some cases the recovery strategies are adequate (green cells) while in most other cases the strategies are inadequate (red cells). Closer inspection yields the following observations:

- Comparing the first and last columns of the map we notice that on disruption, Satellite, is adequately mitigated (average $SDCI_{D,M} < \alpha$).
- Six disruptions have been inadequately managed (average $SDCI_{D,M} > \alpha$ and average $SDCI_{D,M} < SDI_D$)
- The strategies have no effect on one disruption, disruption of Satellite, UAV, and Helicopter.
- The strategies do not address six disruptions (rows with all grey cells). However, two of these disruptions (disruption of the UAV alone and of the Ship's propulsion system) originally had very little impact on the SoS, as seen by their SDI_D values, and hence need not be targeted for resilience improvement.
- The last row in the resilience map provides a summary of the mitigation effectiveness of each strategy (average $SDMI_{D,M}$). The higher this value, the greater the contribution of the mitigation to SoS resilience. Note that repairing the UAV and using better weapons on the Ship have relatively minor mitigation impacts.

Now, how does the resilience map guide decision-making in the context of the naval warfare SoS? Before we answer this question, we first attempt to determine if changing the value of α allows us to focus on a smaller set of red cells to make design improvements rather than considering all ten of them.

Recall that each red cell in the map indicates inadequate resilience. Instead of immediately considering all ten red cells, we vary α to determine how sensitive the colors

in the map are to the risk the decisions maker is willing to accept. This step allows us to prioritize resilience improvement strategies – cells that remain red across a range of α must be addressed first. Returning to the definition of α, we now consider a lower minimum acceptable mission success rate, 50%. Correspondingly, $\alpha = 0.35$. Figure 5.6 shows the resilience map for this new value of α. Unfortunately, varying the decision threshold has not aided the design process – while two cells have turned a lighter shade of red, many of the previously bright red cells remain unchanged.

To guide decision-making we return to Figure 5.5 and list key observations, describe the problems or opportunities they indicate, and point to potential design principles (refer to Table 3.3) to address them.

1. **Observation:** Red cells in column "Better weapons on Ship" indicate that the corresponding disruptions are not adequately mitigated.

   Specific problem: The mitigation measures (i.e., weapons on the Ship) have insufficient range to eliminate threats in the event of an Helicopter disruption.

   Potential solution: *Physical redundancy* can improve the capacity of the mitigation measures. One way to realize physical redundancy is to maintain a backup Helicopter on the periphery of the mission that can be deployed as necessary.

2. **Observation:** The grey cells in average $SDCI_{D,M}$ column indicates that none of the mitigation measures address four disruptions all of which involve a disruption of the Ship's communication system.

   Specific problem: The remaining systems are unable to communicate with each other, meaning any mitigation measures cannot be accessed due to lack of communication capabilities.

   Potential solutions: *Inter-node interaction* can increase communication links between systems. Some ways to realize this principle include:

   - Provide capability for Helicopter to receive information directly from the Satellite if the Ship is disrupted. Resources needed to implement this

recovery feature include increased bandwidth allocation and modifications to communication ports.

- If the Ship is disrupted, provide capability for UAV to receive information directly from the Satellite and in turn for the Helicopter to communicate with the UAV. Resources needed to implement this recovery feature include increased bandwidth allocation and modifications to communication ports.

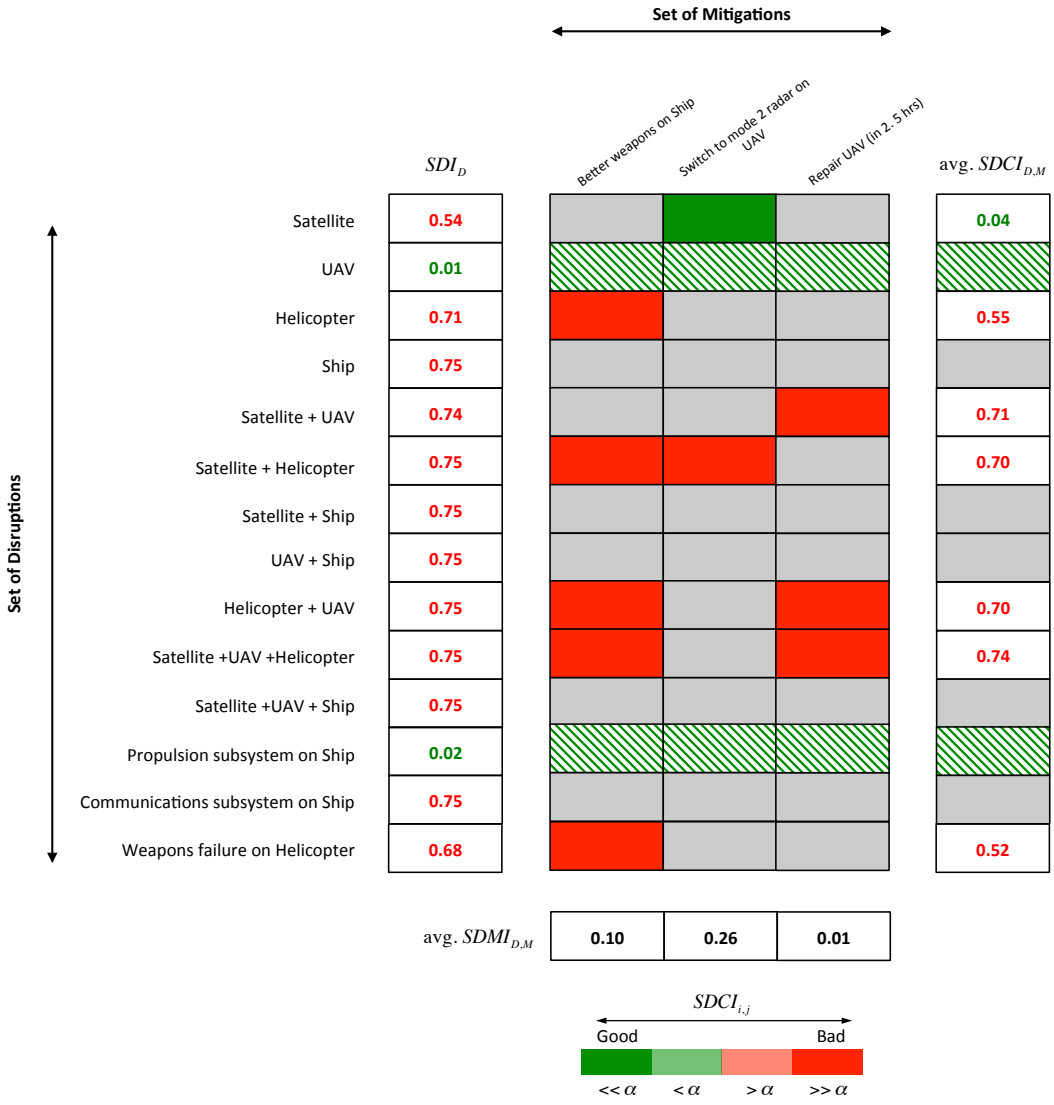

Figure 5.5 Phase 3 Resilience Map for naval warfare SoS ($\alpha = 0.27$)

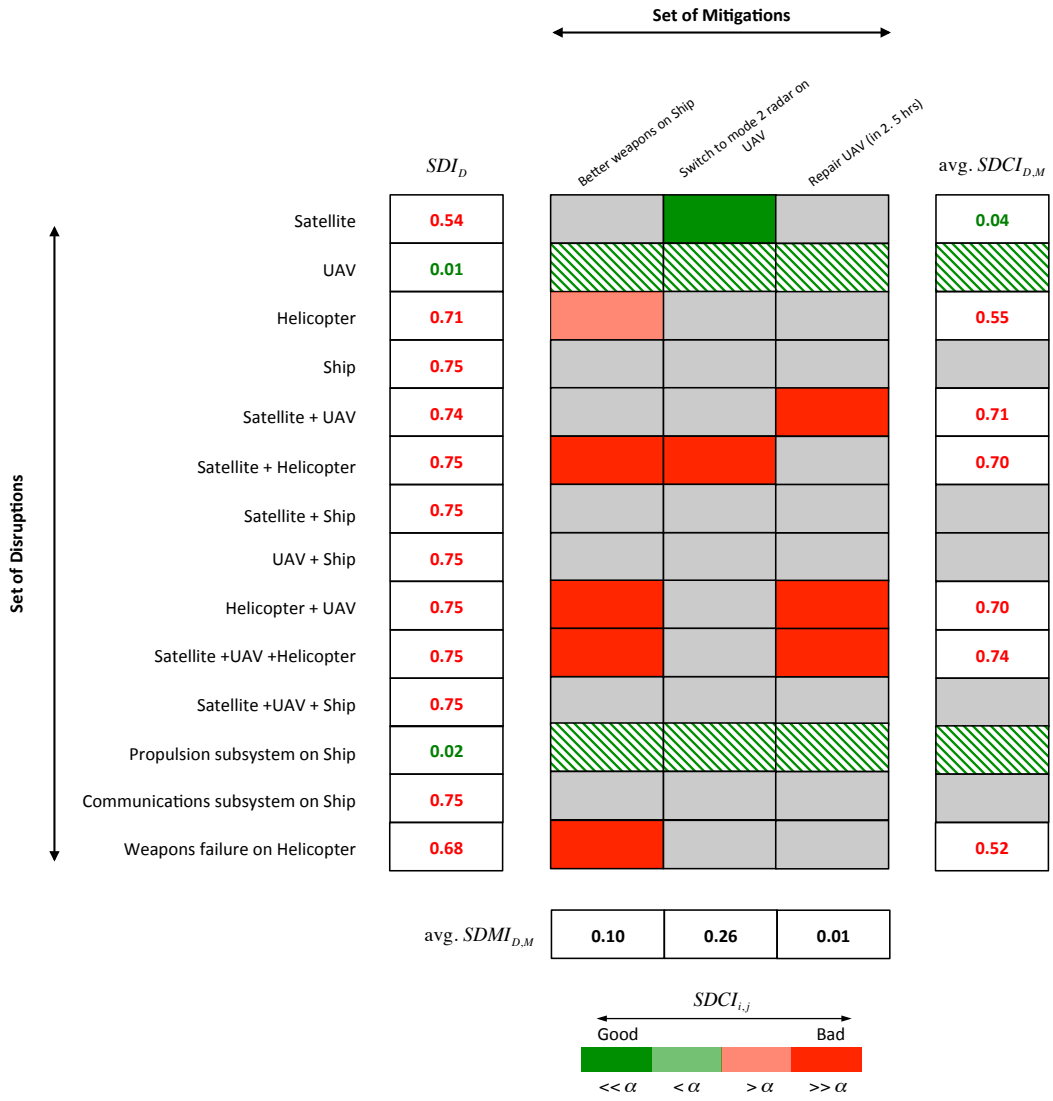

Figure 5.6 Phase 3 Resilience Map for naval warfare SoS ($\alpha = 0.35$)

5.1.4 Phase 4: Improve SoS Resilience

By using the agent-based model to implement the design suggestions from Phase 3, we obtain the new resilience map (see Figure 5.7). On the one hand, clearly the design instances of the inter-node interaction principle are quite effective at mitigating the disruptions of the Ship's communication systems. On the other hand, the backup

Helicopter is no better at addressing the Helicopter disruption than incorporating advanced (better) weapons on the Ship.

From this new map, we conclude that the most pressing disruptive impact that needs to be addressed is the disruption of the Helicopter. Potential suggestions include:

- Improve weapons on Ship: increase the range and/or accuracy of the weapons.
- Improve back-up Helicopter: use a faster helicopter or perhaps even a different one.

Two interesting observations arise from considering the last row (average $SDMI_{D,M}$ values) in the resilience map. First, we can pinpoint those mitigations that contribute significantly to overall resilience, that is, measures with a high average value, and subsequently ensure that these mitigations are available and ready to be deployed when needed. Second, by focusing on those measures that have high average $SDMI_{D,M}$ values, we propose that one way to improve resilience is to combine some or all these highly-effective mitigations so that the resulting "super-set" mitigation strategy is effective across a range of disruptions.

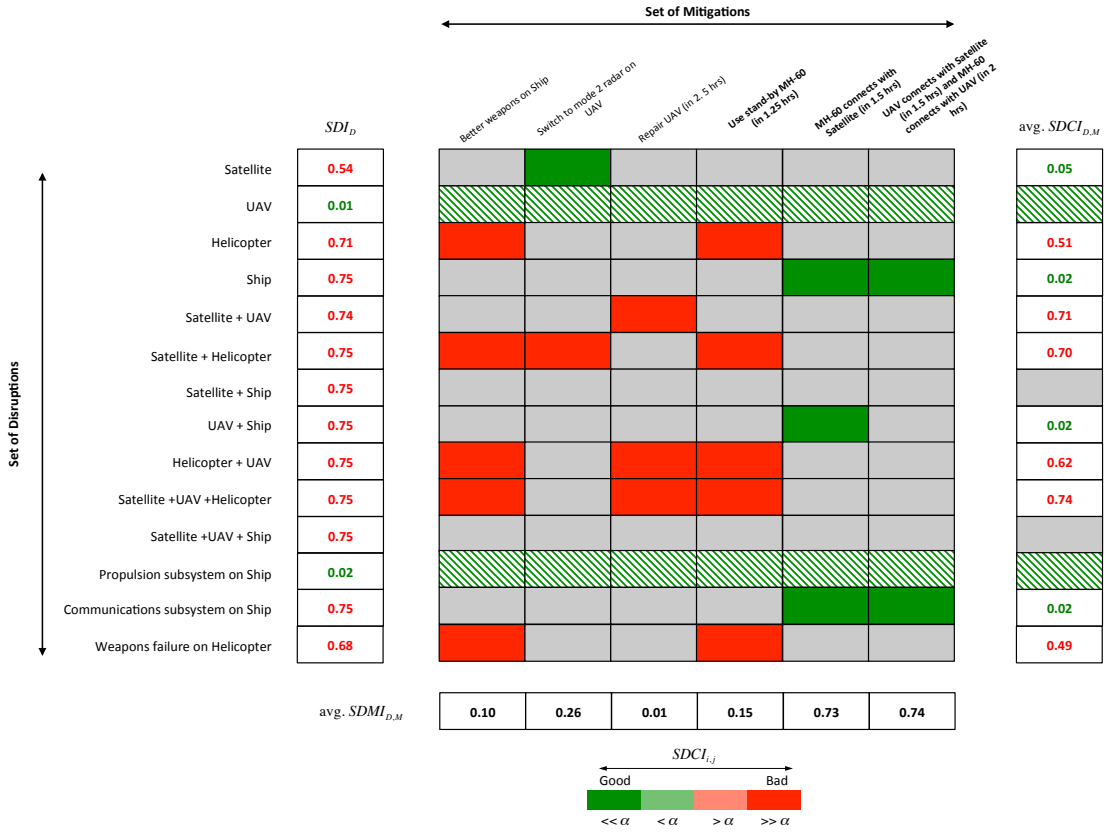

Figure 5.7 Phase 4 Resilience Map for naval warfare SoS ($\alpha = 0.27$)[3]

5.1.5 Summary of Case Study 1

The SIM-based resilience design approach has application to the evaluations of military SoS, as evidenced by the naval warfare case study. Apart from the specific results highlighted in the previous section, broader findings of the case study include:

1. **SIM-based design provides a structured approach to resilience management.** Using the design framework, decision-makers are guided through the analysis of SoS resilience in a systematic way, starting from the identification of disruptions to iterating in a group setting to improve SoS resilience.
2. **Resilience map presents both high-level and detailed information about SoS resilience.** The SIM values as well as color–coded elements within the map

[3] *Caveat*: All times of recovery are relatively conservative and have been chosen to highlight the impact of late recoveries on the SoS.

present specific visual guidance on where the SoS is lacking resilience and where resilience is adequate.

5.2 Case Study 2: Urban transportation SoS

Infrastructure SoSs such as water, power, and transportation provide important services to urban populations. Disruptions of these services have serious consequences for public safety and mobility. For example, Hurricane Sandy impacted electric, communications, and transportation services in New York City for several days in 2012 [NYC, 2013]. While studies have called for an integrated approach to manage the resilience of the nation's critical infrastructure networks, (e.g., NIPP [2006] and PPD [2013]), a recent GAO assessment [GAO, 2014] of the various resilience assessment tools and models used by sub-agencies and contractors of the Department of Homeland Security (DHS) highlights drawbacks of current approaches. For instance, the report states that at present DHS is "not well positioned to integrate relevant assessments to identify priorities for protective and support measures". Also, there is a lack of guidance in terms of ensuring that "the areas that DHS deems most important are captured in [these] assessment tools and methods". In other work, Righi et al. [2015] emphasize that to advance the state of resilience engineering, researchers and practitioners need practical guidance on how "descriptions" of resilience can be translated into "prescriptions". Clearly a key gap in managing resilience is the lack of a structured way to bring together information from different resilience assessment tools and to subsequently motivate resource allocation. We argue that the SIM-based design framework provides a step in this direction.

To highlight how the proposed approach can be used to obtain meaningful information and guide decision-making, we provide a partial resilience assessment of Boston's urban transportation network. As mentioned previously, the purpose of this case study is to illustrate the usefulness of the information that can be gleaned from the results of the resilience framework. We provide a brief discussion on methods that can be used to

determine the relevant inputs (resilience curves and potential disruptions), and then offer a detailed description of the design guidance obtained from the resilience maps.

5.2.1 Determining Potential Disruptions and their Impacts

The Massachusetts Bay Transportation Authority (MBTA) oversees the fifth largest mass transit system in the United States. To provide service within the city, the Authority maintains the following modes of transportation: (1) rapid transit using heavy rail, light rail, and streetcars, (2) commuter rail (typically connecting the city center to the suburbs) using locomotives and coaches, (3) bus service, and (4) commuter boat that provides ferry rides between various points in inner Boston harbor. Figure 5.8 provides an overview of the urban transportation network in Boston.

Figure 5.8 Overview of Boston Urban Transportation SoS [MBTA, 2014a]

Different types of instigating events can disrupt transportation services in a city. For instance, instigating events can be organization-related (e.g. strikes by bus drivers and ticket takers), weather-related (e.g. snowstorms and hurricanes), due to mechanical failures (e.g. power loss and brake failures), or terrorist attacks. These events can cause a wide range of disruptions. For example, a mechanical failure may only impact one bus or one train, while a snowstorm can ground multiple modes of transportation.

The task of identifying potential disruptions can be carried out by a team of analysts and using relevant methods such as brainstorming in a group setting and by leveraging

historical data (e.g. age of vehicles, maintenance data, weather information, policy changes) to determine a list of potential disruptions.

Next, for an urban transportation network, there are several ways to assess the impacts of unmitigated and mitigated disruptions. Examples include simulation software, analytical models, and statistical estimation techniques. Most authorities that oversee the transit services either have in-house tools that are used to carry out various studies regarding network level metrics such as on-time performance and average delays, or have such evaluations carried out by consultants (e.g. RAILSIM software [SYSTRA, 2014]). Additionally, transportation related research has resulted in models that specifically simulate urban transit services (see for example, Balakrishna et al. [2008] and Koutsopoulos and Wang [2007]) Similar to our use of the agent-based model in the previous case study, these simulation tools and analytical models can be directly leveraged to assess the impacts of different disruptions.

A popular metric of interest to quantify SoS level performance in urban transportation networks is **unlinked passenger ridership**, that is, the number of passengers who board public transportation vehicles [MBTA, 2014b]. Passengers are counted each time they board vehicles irrespective of the number of vehicles they use to travel from their origin to their destination. Table 5.4 summarizes typical passenger ridership on weekdays as published by the MBTA [2014b].

Table 5.4 Typical weekday ridership in 2013 on the select modes of transportation in Boston [MBTA, 2014]

Mode	Line	Typical Weekday Ridership
Subway	Red Line	272,684
	Orange Line	203,406
	Blue Line	63,225
	Green Line	227,645
Bus	Silver Line	29,839
	Trackless Trolley	11,588

Mode	Line	Typical Weekday Ridership
	Bus	346,388
Commuter Boat	Ferry	4439

5.2.2 Reading the Resilience Map

In this section, we discuss pertinent information that can be obtained from resilience maps of the Boston urban transportation network. Assuming we have determined the values of the SIMs using the equations presented in Chapter 4, we then use example resilience maps to indicate how resilience-related design improvements can be made.

First, a note about determining an initial decision threshold for urban transportation networks. In these SoSs, α can be specified as the product of two parameters: (1) minimum acceptable SoS performance level, and (2) maximum acceptable time to mitigation. These parameters can be estimated as follows:

1. The first parameter is driven by the specific measure used to evaluate SoS performance. For example, if the SoS performance is measured as passenger ridership, the decision-maker can specify a minimum acceptable level of ridership that the SoS needs to satisfy in the event of a disruption.
2. The second parameter can be estimated in different ways based on stakeholder preferences. For example, one approach is to study historical data and determine how long, on average, are passengers willing to wait after a disruption (see, for example, Kaufman et al. [2012]).

Figure 5.9 shows a partial resilience map with some subset of the total disruptions and a subset of potential mitigation measures. This map explores the state of SoS resilience when certain modes or lines of transportation are disrupted and how well the remaining transit services handle the spillover ridership. We assume here that the SoS here does not provide any explicit means (e.g., shuttle buses) to transport stranded passengers to other links. Hence, the only factors driving the effectiveness of the mitigation strategies are

proximity to the disrupted line and ability of alternate modes to handle the extra passenger traffic.

For example, when the Orange Line (south) is disrupted, three alternate modes of transit (Silver Line, buses in Zone 3, and the commuter rail in Zone 3) are able to partially mitigate the impact. The commuter rail is quite effective in handling spillover traffic from the Orange Line (as indicated by the dark green cell) since it runs parallel to the disrupted line and has several stations collocated with those of the Orange Line. Thus, the passengers who intended to travel on the disrupted Orange line have relatively easy access to an alternate mode of transportation. However, the other two mitigation modes of transport (Silver Line and the bus service in Zone 3) are less effective in mitigating the impact of the disrupted subway line as (1) they do not run the length of the Orange Line and hence do not serve the same locations, meaning passengers would be delayed or inconvenienced with respect to getting to their final locations, and/or (2) they do not have sufficient capacity to handle the extra demand from the Orange Line.

How does the resilience map guide decision-making in the context of the urban transportation SoS? We list key observations, describe the problems or opportunities they indicate, and point to potential design principles (refer to Table 3.3) to address them.

1. **Observation:** Average $SDCI_{D,M}$ values in red indicate that the corresponding disruptions are not adequately mitigated.

   Specific problem (a): The mitigation measures (i.e., alternate transportation modes) have insufficient capacity to handle the spillover demand.

   Potential solutions: *Physical redundancy* and *functional redundancy* can improve the capacity of the mitigation measures.

   - One way to realize physical redundancy is to maintain spare subways and buses, which can be called in to service when there is a disruption on the respective lines.
   - Functional redundancy for disrupted subway lines can be realized by using "bus bridges" [Kepaptsoglou and Karlaftis, 2009]. Bus bridges provide

short-term bus routes between rail (subway or commuter) stations in the event of a disruption. Buses can be mobilized from depots (spare buses) or retracted from existing routes to establish the bus bridges.

An **opportunity** that arises from considering both principles (physical and functional redundancy) is the ability to combine mitigations across multiple transportation modes. For instance, investment in spare buses (a relatively cheaper option than investing in spare trains) is useful to address bus disruptions (deploy the spare bus when a primary bus is disrupted – *physical redundancy*) as well as rail disruptions (deploy spare buses to establish bus bridges between subway stations – *functional redundancy*).

Specific problem (b): Passengers have limited access to these alternate modes.

Potential solutions:

- *Inter-node interaction* can improve access to the mitigation measures. This principle can be realized by providing shuttle services to the nearest alternate mode of transportation (e.g., from the disrupted subway stations to the nearest bus or commuter rail facilities). Another method to increase inter-node interaction is to improve bicycle infrastructure. Suitably located bicycle stations can allow some passengers to cycle to the nearest alternate mode.
- *Improved communication at the organizational level* can improve access to the mitigation measures. Well-established emergency plans that clearly facilitate timely and effective sharing of information between regulatory authorities, operators, and passengers can help minimize performance impacts on the transportation network. Thus, passengers can be evacuated safely and re-directed to other modes of transport efficiently.

2. **Observation:** The presence of red and green cells in columns *Commuter Rail Zone 1* and *Commuter Rail Zone 2* indicate that commuter rail services in both these zones provide adequate mitigations in some instances and inadequate mitigation in other instances. For example, the commuter rail line in Zone 2

provides effective partial recovery when the Orange Line (North) is disrupted but not when the Blue Line is disrupted.

Specific problem: The alternate modes are unable to provide adequate mitigation because passengers have limited access to them.

Potential solutions: *Inter-node interaction* can improve access to the mitigation measures.

- One way to realize this principle in Zone 1 is to maintain bus stops within walking distance of commuter stations. However, making this change would require a redesign of existing bus routes so that the stops are co-located with rail stations. A relatively cheaper option is to provide shuttle services between bus stops and the commuter rail stations. However, this option needs pre-planning in terms of personnel co-ordination and the availability of shuttles to be deployed in a timely manner.
- The principle of inter-node interaction can be realized in Zone 2 by co-locating subway and rail stations. In fact, this design is already seen on the Orange Line (North) where several transfer facilities are provided between commuter rail service and subway stations. Such a provision allows passengers to switch modes relatively easily. Again, since this might be a challenging change to make in the SoS design (extensive structural and procedural modifications of the transit services are required), operating shuttle buses between the stations of the two modes may be a more cost-effective option.

3. **Observation:** The presence of multiple red cells in column *Ferry* indicates that this service contributes inadequately to mitigating the impacts of multiple disruptions.

   Specific problem: While it seems that this mode can be leveraged to mitigate disruptive impacts across several (more than three) adverse events, the passenger capacity of the Ferry service is insufficient.

Potential solution: *Physical redundancy* can improve the passenger ridership capacity of the mitigation measures. One way to realize this principle in this instance is to maintain spare ferries, which are called in to service when there is a disruption. For example, in the aftermath of Hurricane Sandy in New York, an extra ferry was introduced between Manhattan and Staten Island to compensate for the railway disruption [Kaufman et al., 2012].

4. **Observation:** Commuter rail in Zone 1 can mitigate disruption of the Green Line (B), while the Green Line (B) mitigates the disruption Red Line (North).
   Opportunity: It may be possible to improve the SoS design such that Commuter Rail in Zone 1 can be leveraged to mitigate a Red Line (North) disruption.
   Potential solution: *Inter-node interaction* can facilitate movement of passengers from the Red Line to the Commuter Rail. As before, timely shuttle services can provide the required transfer capabilities between the disrupted subway and mitigating rail modes.

5. **Observation:** The grey cell in average $SDCI_{D,M}$ column indicates that none of the mitigation measures address the disruption of Green Line (D).
   Specific problem: Passengers affected by the disruption are unable to access alternate transit modes.
   Suggested improvement: The resilience map does not point to specific improvements. The decision-maker needs to carefully study the reasons for the current inability to mitigate this disruption and identify potential mitigation measures.

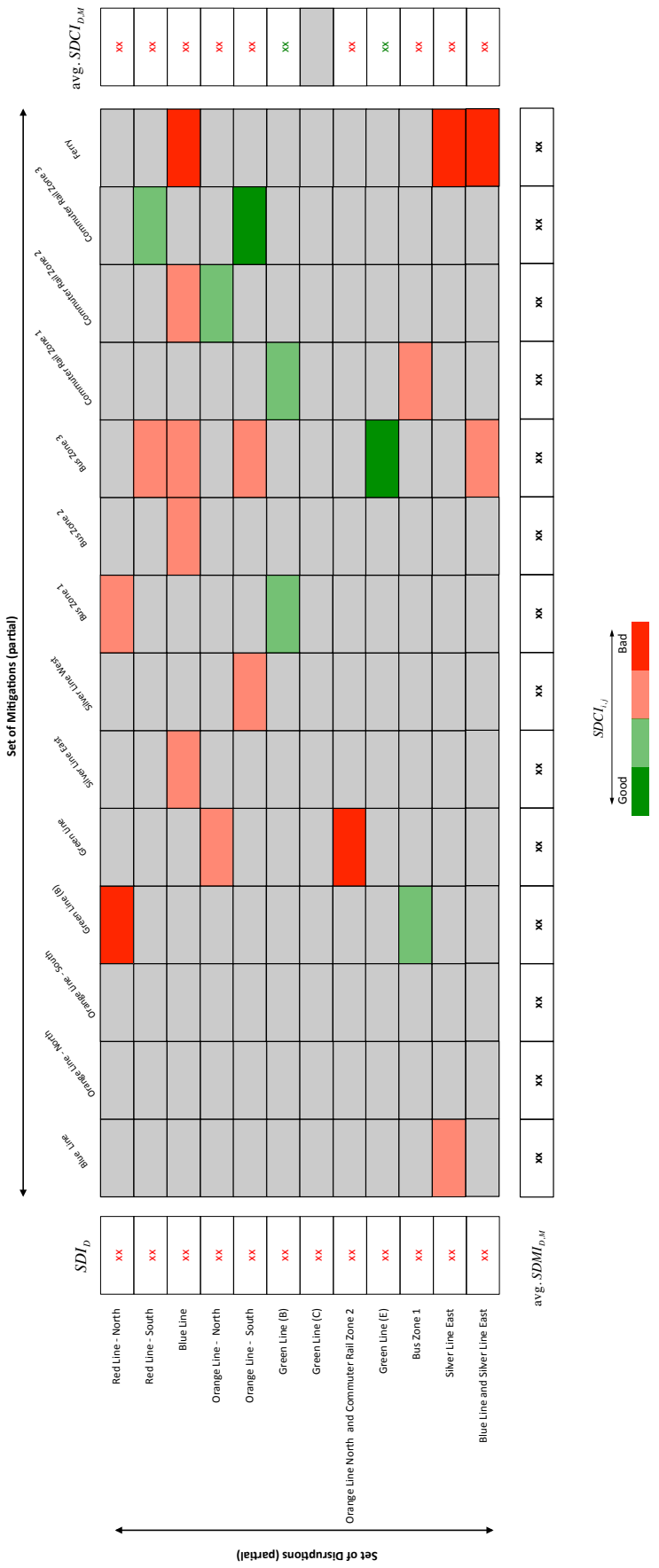

Figure 5.9 Example Resilience Map (partial) for Boston urban transportation SoS

Figure 5.10 shows another example of a partial resilience map for the Boston urban transportation SoS. This map reflects a more resilient SoS with better mitigation measures that have been realized, for example, by implementing the functional redundancy and inter-node interaction suggestions from the previous discussion. Now, how does this resilience map guide decision-making for the SoS? As before, we list key observations, and then point to potential design principles to address them. However, here, we do not discuss implications of red cells in the map. These cells can be interpreted in a similar fashion as the previous resilience map. Instead, we focus on the green cells and describe the opportunities they suggest for resilience improvement.

1. **Observation:** The presence of light green cells in the mitigation columns for bus service (Zones 1, 2, and 3) and commuter rail (Zones 1, 2, and 3) indicate that these two modes are reasonably well equipped to provide mitigation when disruptions occur.

   Opportunity: While many of the cells are light green, there is room for further improvement (that is, to make them dark green), ensuring even better mitigation of the disruptions. However it may be the case that we have reached maximum feasible effectiveness in terms of additional capacity to carry passengers and providing passengers with access to these alternate modes. In such situations, one way to improve the resilience further is to focus on delaying or reducing the impact of the disruption.

   Potential solutions: *System-level properties* and *drift correction* can improve the capacity of the mitigation measures.

   - One way to leverage system-level properties is to improve the robustness of the subway design by either deploying inflatable flood barriers in subway tunnels or constructing raised entrances at flood-prone stations. Another technique, with a focus on road design, is to upgrade pavements using materials that can withstand extreme weather. This improvement allows continued bus service during winter weather storms.
   - One way to realize drift-correction is to deploy sensors in subway tunnels to detect rising water levels and automatically activate water pumps. Thus,

pre-emptive initiation of mitigation allows subway services to continue for a longer duration of time before being halted than would otherwise be possible.

2. **Observation:** When considered together, the bus service (Bus Zone 1, Bus Zone 2, and Bus Zone 3) and commuter rail (Commuter Rail Zone 1, Commuter Rail Zone 2, and Commuter Rail Zone 3) are able to adequately mitigate all the disruptions in identified set.

Opportunity: A useful next step would be to assess what minimum combination of these six mitigation strategies could be the most effective. For instance, the bus service and commuter rail in Zone 3 sufficiently address the same disruptions. Decision-makers can now explore if either of these can be downgraded slightly in order to allocate resources to transportation facilities in other zones..

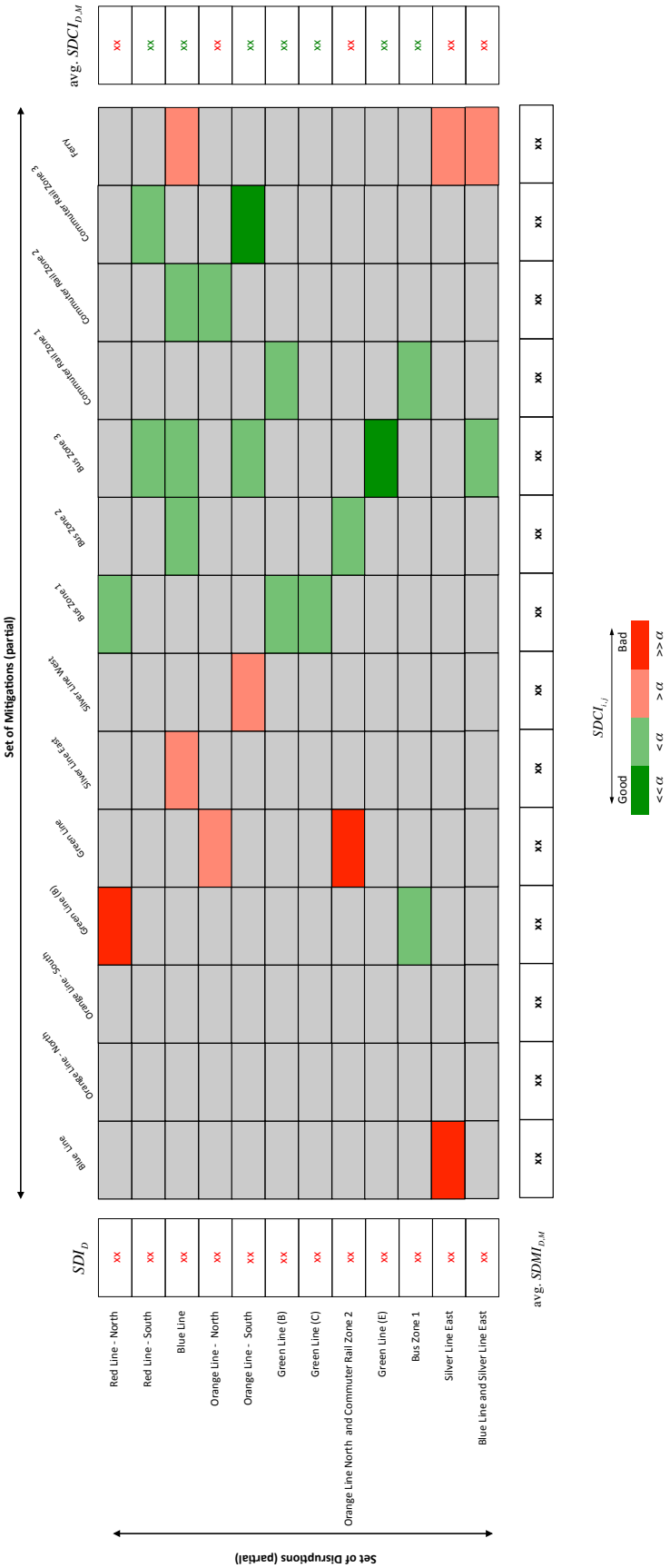

Figure 5.10 Example Resilience Map (partial) for Boston urban transportation SoS

5.2.3 Summary of Case Study 2

The resilience framework has application in resilience management of infrastructure networks such as urban transportation. The design framework provides transit authorities with a systematic approach to evaluating SoS resilience and determining suitable improvements.

Results of a recent survey of 48 international transit agencies [Pender et al., 2013] concluded that many of these organizations do not have adequate parallel transportation networks in the event of subway disruptions. In addition, it was observed that the primary focus of existing mitigation measures is to provide crossover tracks that facilitate the quick removal of the disrupted vehicles and thereby allow spare trains to provide service. While there is consideration of using multiple mitigation alternatives, these measures are typically determined in an ad-hoc manner based on immediate needs of the SoS. For example, in the aftermath of Hurricane Sandy, the MTA implemented a system of "bus bridges" from Brooklyn to Manhattan designed as a substitute for subway lines that cross the East River. However, since at first the operation of these buses was not streamlined, long waits (more than an hour) were reported for subway shuttle buses in Brooklyn [Kaufman et al., 2012]. If instead, the use of these shuttle buses was planned for as part of emergency transportation procedures, it is likely that the operations would have been executed with less delay for the traveling public.

In summary, the SIM-based resilience design can contribute to the development of organizational and contingency plans in the event of disruptions. The resilience map, in particular, helps identify un-resilient modes and point to ways to address them.

CHAPTER 6. CONCLUSIONS AND FUTURE WORK

Systems-of-systems are ubiquitous and here to stay. The services provided by SoSs are typically vital and time-sensitive. It is therefore essential that these networks be made resilient to adverse events. This thesis revolves around the issues of managing resilience in systems-of-systems. A comprehensive treatment of the topic should address the following three questions:

1. What is resilience in the context of an SoS and when is it appropriate?
    - How can resilience be distinguished from other system-level attributes?
2. How can resilience be designed?
    - What level of resilience is desirable and how resilient is the SoS currently?
    - What principles can be applied to achieve resilience in SoS design?
3. How can resilience be maintained over the SoS lifetime?
    - When does resilience change?
    - How can adverse impacts of changing resilience be observed and mitigated?

In this research, we addressed questions 1 and 2. First, we reviewed the concept of resilience as discussed in various domains, and then provided a comparison with related engineering attributes such as reliability, robustness, and flexibility. We argue that characterizing the purpose of the different attributes and in some cases disentangling the definition of resilience from related system-level attributes is useful in enriching overall SoS design.

Next, we focused on the second question: how can SoS resilience be designed? Methods, tools, and processes that can be applied to designing resilient SoSs were categorized and discussed. We observed that while traditional risk and reliability tools have use in assessing resilience, their application has limitations. Instead recent multi-disciplinary research that has made significant strides in modeling and evaluating SoSs can be leveraged more effectively to answer the question. Based on this review, we concluded that the biggest gap is in providing design guidance for resilience and that there exists a need to facilitate informed decision-making at the SoS level.

This thesis has developed an **aid to design** that provides specific guidance on where and how resources need to be targeted. Specifically, we adapted the traditional risk-based design process to include two SoS-focused features. First, system importance measures (SIMs) determine the relative importance of different systems based on their impacts on SoS-level performance. Second, suggestions for resilience improvement draw from design options that leverage SoS-specific characteristics, such as the ability to adapt quickly (such as add new systems or re-task existing ones) and to provide partial recovery of performance in the aftermath of a disruption.

More broadly, the design process:

- **Allows rapid understanding of different areas of concern within the SoS.** The visual nature of the resilience map (a key outcome of the SIM analysis) provides a useful way to summarize the current resilience of the SoS as well as point to key systems of concern.
- **Provides a structured approach to resilience management.** Using the design framework, decision-makers are guided through the analysis of SoS resilience in a systematic way, starting from the identification of disruptions to iterating in a group setting to improve SoS resilience.
- Provides a platform for multiple analysts and decision-makers to **study, modify, discuss and document** options for SoS.

6.1 Recommendations for Future Work

The SIM-based design approach presented in this thesis is one step towards formalizing the resilience design process. The following areas provide promising topics for future work.

6.1.1 Value of Design Improvements

While the resilience framework allows us to determine potential design improvements, the next step is to conduct a suitable analysis of alternatives. One way is to use the SIMs to evaluate the benefit of potential improvements in a traditional cost-benefit analysis. For instance, we can incorporate the marginal cost of implementing a particular mitigation by dividing each system importance measure by the corresponding cost associated with it. Such a SIM/cost metric would allow us to compare different mitigation strategies and determine which ones provide the most mitigation effectiveness for the least cost.

6.1.2 Non-linearity of Performance and Time

The System Importance Measures presented in Chapter 4 assume a linear importance of performance over the course of some time frame. However, this linearity may not always be observed – the performance drop may become less significant as time passes. For instance, as mentioned previously, in some cases providing even poor alternative transportation modes during rush hour may be better than waiting for better modes.

One avenue to address this issue is by using a family of nonlinear functions to represent the temporal and performance level importance of SoS performance.

6.1.3 Broader Application of the Resilience Design Process

The SIMs are domain-agnostic and have a generic formulation based on performance and time. These features permit wider application of the SIMs, for instance, at the system level. Here, while the SIMs can be used to evaluate system resilience, the principles and

design choices that drive resilience improvement are system-dependent. Hence, while the resilience design process remains the same, *how* the design is done is based on system-level considerations.

6.1.4 Uncertainties and Complex Effects

The SIMs presented in this thesis are calculated assuming that a disruption does occur and that the mitigation measure is available to provide temporary recovery. However, in many cases, these two assumptions may not hold and so in this section we discuss how some uncertainties and complex effects can be factored in to the system importance measures.

Expected System Importance Measures (SIMs)

Here, we consider two aspects of uncertainty: the uncertainty regarding the occurrence of a disruption and the availability of a mitigation measure:

1. **Uncertainty in disruptions**. The same instigating event can result in different disruptions. For example, moderate snowfall in Atlanta has a higher likelihood of disrupting Atlanta Hartsfield-Jackson International Airport (ATL) while Chicago O'Hare International Airport (ORD) is reasonably well equipped to handle the same level of snowfall. The likelihood of being adversely affected is not only a function of the disruptive event itself but also of the available resources (infrastructure, emergency personnel, organizational flexibility).
2. **Availability of mitigation measure.** In some situations, mitigation strategies may not be available. For example, a blizzard can impact two airports in a particular metroplex, rendering both unable to handle diverted flights (a mitigation measure which would otherwise have been possible if one airport was disrupted by a hostile attack while the other was not).

To account for the above factors we develop the *expected System Importance Measures.* Now, we can express the outcomes of an instigating event as a decision tree (see Figure

6.1). There are three possible outcomes: the "nominal curve" (refer to Figure 4.8), the "disruption curve" (refer to Figure 4.10), and the "resilience curve" (refer to Figure 4.16). Recall that SDI_D measures the disruption curve, while $SDCI_{D,M}$ and $SDMI_{D,M}$ represent the resilience curve. Also, D is a disruption and M is a mitigation measure.

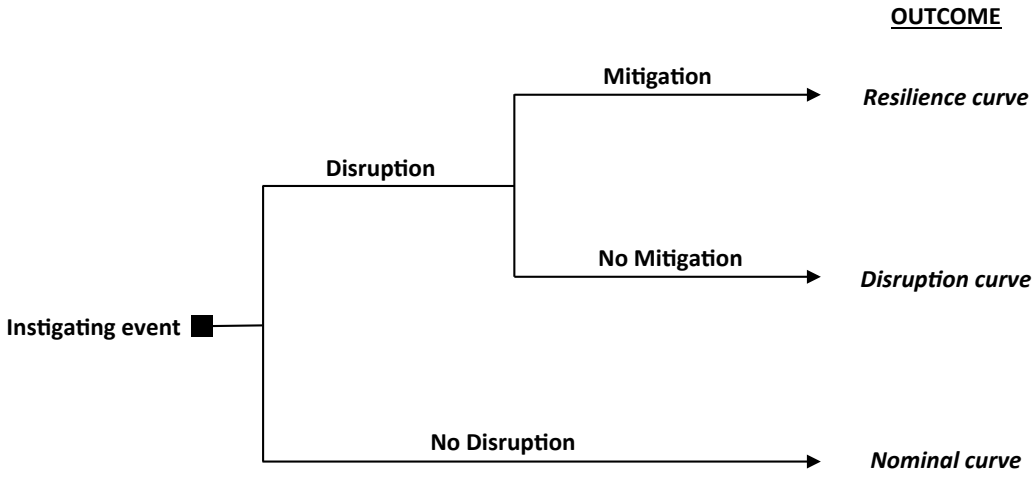

Figure 6.1 Event tree for expected SIMs

Now, referring to the "resilience curve" outcome in the decision tree, the expected value of $SDCI_{D,M}$ can be expressed by eq. (8):

$$E\left(SDCI_{D,M}\right) = SDCI_{D,M} \cdot P(D) \cdot P(\overline{M}|D) \tag{8}$$

Where $P(D)$ is the probability that the disruption D occurs and $P(\overline{M}|D)$ is the probability that the mitigation measure is unavailable given D has occurred

Expanding the conditional probability and if $P(D) > 0$, we obtain eq. (9).

$$P(M|D) = \frac{P(\overline{M} \cap D)}{P(D)} \tag{9}$$

Substituting eq. (9) in eq. (8), the expected value reduces to eq. (10).

$$E\left(SDCI_{D,M}\right) = SDCI_{D,M} \cdot P(\overline{M} \cap D) \quad (10)$$

Now, if D and M are independent events then $P(\overline{M} \cap D) = P(D) \cdot P(\overline{M})$. Thus, the expected $SDCI_{D,M}$ can be expressed as eq. (11).

$$E\left(SDCI_{D,M}\right) = SDCI_{D,M} \cdot P(D) \cdot P(\overline{M}) \quad (11)$$

In many instances, the above equation is reasonable. For example, disruption of subway service in New York City due to flooding of rail tunnels most likely will not affect the ability of extra bus service to compensate for the rail. SoS engineers can use either historical data to determine the disruption and mitigation probabilities, or model them as random variables using appropriate distributions. However, when D and M are not mutually independent, such as in the case of common cause disruptions (a single instigating event causes the disruption of multiple systems) and cascading disruptions (disruption of one system adversely impacts other systems), careful consideration needs to be made to determine the join probability $P(\overline{M} \cap D)$.

Similar to $E(SDCI_{D,M})$, the expected $SDMI_{D,M}$ can be determined as shown in eq. (12):

$$E\left(SDMI_{D,M}\right) = SDMI_{D,M} \cdot P(D) \cdot P(M \cap D) \quad (12)$$

Again, when D and M are independent events, eq. (12) reduces to eq. (13):

$$E\left(SDMI_{D,M}\right) = SDMI_{D,M} \cdot P(D) \cdot P(M) \quad (13)$$

Returning to the resilience design process, if the relevant probabilities are available or can be estimated, Phases 3 and 4 can be carried out using these expected SIMs as before to determine the expected resilience maps.

6.2 Further Considerations for Research in Resilience based on SoS Characteristics

In this thesis, we presented one approach to facilitating decision making in the context of SoS resilience. However, there are several other avenues to advance the state of resilience research. Here we use the characteristics of SoSs to identify design questions and suggest potential research directions, as summarized in Table 6.1.

Table 6.1 Key questions in designing resilient SoSs

SoS characteristic	Specific design questions
Large-scale with heterogeneous systems	• How can sufficiently detailed models be developed that do not over-simplify the problem? • How can models capture cross-domain coupling effectively? • How can the computational challenges associated with large models be dealt with efficiently?
Uncertainties in SoS evolution and operating environment	• How can internal and external uncertainties be modeled? • Where should resilience be added? • Will there be any unintended consequences of resilience improvement measures? • What is an acceptable or suitable level of resilience for a particular SoS?
Multiple stakeholders and/or partial control of SoS	• How can we develop strategies that incentivize and facilitate resilience improvement measures for the overall SoS in a climate of uneven distribution of costs and benefits, and uncertain realization of benefits?

6.2.1 SoSs are typically large-scale networks that consist of a variety of heterogeneous systems

The ability of SoSs to provide capabilities that single systems cannot stems from their inherent diversity, that is, the variety of their constituent systems (heterogeneous nature of SoSs) and, in many cases, the geographical distribution of these systems (large-scale feature of SoSs). While these characteristics are essential to achieving SoS goals, they present challenges that can stymie efforts to effectively analyze SoSs, particularly with respect to modeling SoS resilience. These issues include modeling the interactions within and between SoSs, and computational challenges associated with large models.

All complex systems pose a modeling challenge, which essentially comes down to determining what the minimum level of fidelity is that will still provide useful results (and whether this fidelity is computationally tractable). This problem is especially tough in the case of SoSs, where even low-fidelity models can rapidly become very large and hence computationally challenging and difficulty to verify and validate. Several researchers have been addressing this problem by modeling SoSs as networks, which enables them to leverage network theory. But this approach requires that nodes be identical, or that only a few types of nodes be considered. Other work has extended modeling and measurement efforts to include performance levels of heterogeneous nodes rather than just flows between nodes in a network. However, most of these studies tend to be infrastructure-specific, and hence have limited use. Given the above discussion (see also Section 3.2), it is fair to ask:

How can we develop sufficiently detailed models to analyze SoS resilience?

The first set of research questions relates to developing models of adequate fidelity to analyze SoS resilience. Specifically: (1) How can we develop sufficiently detailed models that do not over-simplify the problem? (2) How we can we efficiently capture cross-domain coupling? and (3) How do we deal with computational challenges associated with large models? Answers to these questions will provide useful contributions to the SoS engineering community. Some routes to solving these questions are:

- **Use pattern recognition to model evolution of SoS operations.** One promising approach is to leverage advances in "Big Data" tools and techniques to the analysis of resilience in SoSs. This method has been used effectively in weather prediction and modeling. Computer software is used to identify previous weather patterns that closely resemble the current conditions, and then the predicted outcome is based on some weighted combination of the previous, similar, outcomes. Similarly, exploring response patterns of existing SoSs to previous disruptions could be used to evaluate new architectures. For example, Kalawsky et al. [2013] use pattern recognition to model emergency response (SoS

comprising police departments, fire brigades, and ambulance services) for a major incident in the UK.

- **Use cloud-based computing to facilitate the development of large SoS models.** Some advantages of using this approach include: (1) the ability to separately develop various aspects of the larger model (co-locating simulations and resources is no longer a constraint), and (2) the ability to involve multiple, distributed contributors and expertise simultaneously (researchers need not "reinvent the wheel": existing models can be used and built upon remotely).
- **Use Meta-models that consider multiple models, multiple experts, and shared variables and parameters to represent and analyze SoSs.** For example, consider the case of a rise in sea level due to climate change and its impact on saltwater intrusion into coastal groundwater aquifer systems. Haimes [2012] describes three system models to analyze this phenomenon: hydrological (water modeling), agricultural-social (impacts on agriculture and domestic water supplies), and regional economic models (economic impacts). All three models draw inputs from the same database (here, external climatological models). In other work, Filippini and Silva [2015] present a modeling language (I®ML) to facilitate analysis of interdependencies with the aim to improve SoS (in particular, critical infrastructure) resilience. The authors also provide a discussion of other useful models, such as the functional resonance analysis model [Hollnagel, 2012] and an interdependency model based on failures and repairs [Johansson and Hassel, 2010]. Carley [2003] presents the concept of Dynamic Network Analysis to evaluate network evolution and change propagation in large-scale, dynamic networks; this approach provides fertile ground for the development of SoS-focused meta-models.
- **Leverage Human-System Integration research to improve SoS design and accessibility for human operators.** As SoSs continue to grow in size and complexity, the integration of humans with software and systems becomes increasingly significant. Currently, human capabilities and limitations and their implications on the design, deployment, operation, and maintenance of SoSs are

typically not explicitly addressed in SoS engineering and acquisition lifecycles [Madni, 2010]. This challenge can be addressed by incorporating human-system integration (HSI) ideas such as cognitive compatibility, identification of HSI patterns, and human performance modeling. For example, one specific ongoing project [Rouse, 2012] explicitly models human behavior and performance as part of a larger effort to improve the application of systems engineering to SoSs.

- **Develop metrics for the price of uncertainty to provide guidance in establishing modeling requirements.** Apart from building SoS resilience models, a key challenge is evaluating the models themselves. Specifically, what level of model fidelity can provide the required quality of guidance to decision-makers? One way to answer this question is through the development of suitable metrics and methods that help assess this price of uncertainty.

6.2.2 SoSs operate in environments of high degrees of uncertainty

Traditionally, system optimization has sought to identify the "best" point design given a fixed set of constraints for the entire lifetime of the system. However, in the case of long-lasting SoSs, such as infrastructure and transportation networks, this approach of deterministic optimization over a single period cannot be solved in a permanent sense. The key hurdle to identifying an optimal solution is the uncertain environment, both endogenous (internal) and exogenous (external), in which SoSs typically operate. Endogenous uncertainty includes SoS evolution in terms of phasing out of old systems, inclusion of new systems, upgrades to existing systems, and changes to the underlying communication (cyber). Exogenous uncertainty is driven by changes in the external environment, such as new types of threats, new requirements to interface with other SoSs, and changing stakeholder needs. Further, this uncertainty ranges from the well-defined (e.g., we know that Boston will most likely experience several blizzards every winter), to the much more difficult "unknown-unknowns". So, the second set of research challenges stem from the following question:

Given the uncertainties in hazards, technologies, and SoS structure, how can we make SoSs optimally resilient?

The uncertainties mentioned above have a significant impact on modeling and managing SoS resilience. Specific questions that decision-makers need to address include: (1) How can internal and external uncertainties be modeled? (2) Will there be any unintended consequences of resilience improvement measures? and (3) What is an acceptable or suitable level of resilience for a particular SoS? An SoS that is optimally resilient now to a certain class of threats may not be optimally resilient in the future as its constituent systems and the external threats change in time (there is also the question of what "optimally resilient" means). For example, in recent years airports have been made more resilient to terrorist attacks (through improved screening and emergency response procedures). However, as global-warming induced changes affect weather patterns, these airports may not be resilient to blizzards and rainstorms that may occur with higher frequency in the future. Also, specifically with respect to infrastructure SoSs, engineers and designers seldom have the opportunity to design an SoS "from scratch" – these SoSs typically evolve over many decades as systems are acquired, upgraded, and/or removed. And so a fourth question arises: is it possible to upgrade a formerly un-resilient SoS into a resilient one?

Addressing unforeseen changes is a challenging task primarily because identifying "unknown unknowns" by definition is impossible. However, while we do not always know why or how systems and processes might be disrupted, we can improve anticipation and recovery efforts through improved SoS modeling. For example, tools that facilitate the analysis of multi-system failures are valuable in directing resilience improvement resources. Similarly, as it is likely that different systems will come back online at different times (e.g., refer to previous example of impact of different rate of recovery of aviation and rail transportation in New York city in the aftermath of Hurricane Sandy), such tools would be useful to mitigate the harmful impact of asynchronous recoveries.

These situations highlight the need for discussions about the acceptable level of resilience an SoS needs to maintain and over what range of scenarios this resilience should be available. Another factor that has significant implications for managing resilience under uncertainty is the inherently multi-dimensional aspect of resilience: performance and time. As a result, in many cases decisions about resilience improvement must consider where the resilience should be placed, that is, following a disruption, should we improve the performance considerably albeit after a significant downtime or should we ensure a timely recovery with minimum performance recovery?

We believe that the abovementioned challenges offer opportunities to "creatively" tackle the issue of SoS resilience, and here, suggest a few ways to approach this thorny challenge:

- **Identify "resilience pathways" that allow an SoS to remain resilient over long time periods.** As threats and the constituent systems of the SoS evolve stochastically over the lifetime of the SoS, the necessary optimization must put the SoS on a "path to resilience", that is, it must allow for incremental changes that can maintain resilience of the SoS over time.
- **Use the concept of multiple equilibria from ecology to design engineering resilience.** As the interdependencies between SoSs, and not just between their constituent systems, grow, the concept of multiple equilibria from ecology (ability of a system to move into a different equilibrium or stable state to maintain functionality in the face of a disruption [Holling, 1973]) could provide an interesting approach to developing resilient SoSs. For example, can we design transportation networks that allow demand to be shifted over and sustained on the bus networks in the event of a major railway disturbance, thereby shifting the "equilibrium" from rail to road? These studies would need to also take into account social behavior and preference patterns of the general public, further strengthening the idea that multiple disciplines as widely diverse as engineering and psychology, for example, would need to be corralled to analyze SoS resilience in its entirety [Jackson, 2007].

6.2.3 SoS operations involve multiple stakeholders and in many cases partial control over the SoS

The constituent systems in most civilian SoSs, such as infrastructure and transportation networks, are typically owned and operated by different entities and/or organizations. Similarly, in the military domain, although SoSs exhibit a defined structure with respect to their operations, a variety of stakeholders are involved in the development of the constituent systems. Hence, attempts to improve the resilience of SoSs may result in situations where some stakeholders are required to accept greater costs. The following question drives the third set of research challenges:

How can we develop strategies that incentivize and facilitate resilience improvement measures for the overall SoS in a climate of uneven distribution of costs and benefits, and uncertain realization of benefits?

Since the human element is a significant part of the development, operation, and maintenance of resilient SoSs addressing the above question can improve discussions about resilience improvement strategies. Some suggestions are provided below:

- **Develop tools to support decision-making and information exchange between stakeholders.** From a technological perspective, better decision-making tools that support stakeholder collaboration efforts are needed to improve the quality of resilience-related discussions. These tools can be developed by adopting recent advances in fields such as collaboration technology, information abstraction, visual analytics, and data sharing [Provan and Kenis, 2008; Neches and Madni, 2012]. Additionally, existing frameworks such as DoDAF [DoD, 2010] and the Open Group Architecture Framework (TOGAF) [Open Group, 2011] can be leveraged to facilitate SoS visualization and communication between analysts and stakeholders.
- **Improve stakeholder risk perception through the development of risk communication tools.** For the overall SoS to be made resilient, some fraction of

the constituent systems must include features to mitigate effects of disruptions. This uneven spread of resilience requirements implies a disproportionate spread of stakeholder benefits and costs. Further, the value of a particular resilience strategy is only realized when the disruptions or failures actually occur. As a result, improved risk communication tools need to be developed (as highlighted in Aven [2013b]) to improve risk perception and to help stakeholders make decisions.

- **Develop common standards to facilitate SoS development.** Just as common standards enable the concurrent but separate development of subsystems (e.g., testing standards ensure that all subsystems meet minimum electromagnetic compatibility requirements), common standards may enable multiple stakeholders to work together more effectively to develop systems-of-systems. Obvious standards include selecting SI or English units—however, could more sophisticated standards be helpful? For example, would using the System Modeling Language (SML) contribute to faster or otherwise more effective development? Similarly, do the lessons and benefits of concurrent engineering transfer to SoS level engineering?
- **Develop strategies to minimize cost-benefit imbalances to stakeholders.** Resilience improvement measures at the SoS-level can result in an uneven distribution of costs and benefits across stakeholders, which may make some reluctant to participate. Given these potential imbalances, new approaches are needed to determine which strategies are most appropriate to persuading stakeholders to make the necessary changes or upgrades to their systems. For example, Marais and Weigel [2006] present a framework to encourage successful technology transition in civil aviation. Specifically, the authors use cost, benefit, and value distributions across stakeholders and over time to determine which strategies are most appropriate to persuading aircraft operators to adopt new equipage. Specific strategies could include phased implementation of resilience improvement measures, positive incentives such as monetary benefits or tax breaks to early participants, and mandates and punitive approaches.

LIST OF REFERENCES

LIST OF REFERENCES

Abbott, R. (2006). Open at the Top; Open at the Bottom; and Continually (but Slowly) Evolving. *IEEE International Conference on System of Systems Engineering.* Los Angeles, CA.

Albert, D. S. and Hayes, R. E. (2003). Power to the edge. *DOD Command and Control Research Program (CCRP).* URL: http://www.dodccrp.org/files/Alberts_Power.pdf. Accessed March 01, 2014.

Alessandri, A. and Filippini, R. (2013). Evaluation of Resilience of Interconnected Systems Based on Stability Analysis. *Lecture Notes in Computer Science*. Vol.7722. pp:180-190.

Attoh-Okine, N., Cooper, A. T., and Mensah, S. A. (2009). Formulation of resilience index of urban infrastructure using belief functions. *IEEE Systems Journal*. Vol. 3(2), pp: 147- 153.

Ash, J. and Newth, D. (2007). Optimizing Complex Networks for Resilience Against Cascading Failures. *Physical Review A*. Vol. 380. pp: 673–683.

Aven, T. (2013a). Practical implications of the new risk perspectives. Reliability Engineering and System Safety. Vol. 115. pp: 136-145.

Aven, T. (2013b). On How to Deal with Deep Uncertainties in a Risk Assessment and Management Context. Risk Analysis. Vol. 33(12). pp: 2082-2091.

Ayyub, B. (2014). Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision-Making. *Risk Analysis*. Vol. 34(2). pp 340-355.

Balakrishna, R., Wen, Y., Ben-Akiva, M., and Antoniou, C. (2008). Simulation-Based Framework for Transportation Network Management in Emergencies. *Transportation Research Record: Journal of the Transportation Research Board*. Vol. 2041(1). pp: 80-88.

Barabási, A-L. and Albert, R. (1999). Emergence of scaling in random networks. *Science*. Vol. 286. pp: 509-512.

Barker, K., Ramirez-Marquez, J. E., and Rocco, C. M. (2013). Resilience-Based Network Component Importance Measures. *Reliability Engineering & System Safety*. Vol. 117. pp 89-97.

Barker, K. and Baroud, H. (2014). Proportional hazards model of infrastructure system recovery. *Reliability Engineering and System Safety*. Vol. 124. pp: 201-206.

Barkhorn, E. (2014). Map: 'How Much Snow It Typically Takes to Cancel School in the U.S'. *The Atlantic.* URL: http://www.theatlantic.com/education/archive/2014/01/map-how-much-snow-it-typically-takes-to-cancel-school-in-the-us/283470/. Accessed March 26, 2015.

Barot, V., Henshaw, M, Siemieniuch, C., Sinclair, M, Lim, S. L., Henson, S., Jamshidi, M., and DeLaurentis, D. (2013). SoA Report. *Trans-Atlantic Research and Education Agenda in Systems of Systems (T-AREA-SoS)*. URL: https://www.tareasos.eu/docs/pb/SoA_V3.pdf. Accessed March 10, 2014.

Bartelt, D. (1994). On resilience: questions of validity. In Wang, M. and Gordon E. W. eds. *Educational Resilience in Inner-city America: Challenges and Prospects*. Lawrence Erlbaum. Hillsdale, NJ.

Barker, K. and Baroud, H. (2014). Proportional hazards model of infrastructure system recovery. *Reliability Engineering and System Safety*. Vol. 124. pp: 201-206.

Ben-Haim, Y. (2012). Why risk analysis is difficult, and some thoughts on how to proceed. *Risk Analysis.* Vol. 32(10). pp: 1638-1646.

Bowen, J. and Stavridou, V. (1993). Safety-critical systems, formal methods and standards. *Software Engineering*. Vol. 8(4). pp:189-209.

Brown, R. and Drew, C. (2012). Airlines Begin a Laborious Comeback. *New York Times* (October 31) . URL: http://www.nytimes.com/2012/11/01/business/after-hurricane-sandy-returning-to-the-air.html?pagewanted=all. Accessed January 09, 2014.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., and von Winterfeldt, D.(2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra.* 19(4), pp: 733–752.

Bruneau, M. and Reinhorn, A. (2004). Seismic resilience of communities—Conceptualization and operationalization. *International Workshop on Performance-based Seismic Design*. Bled, Slovenia. June 28–July 1.

Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., and Havlin, S. (2010). Catastrophic Cascade of Failures in Interdependent Networks. *Nature*. Vol. 464. pp: 1025–1028.

Carley, K. M. (2003). *Dynamic network analysis. Dynamic Social Network Modeling and Analysis:Workshop Summary and Papers*. pp:133-145

Castet, J-F. and Saleh, J. H. (2012). On the concept of survivability, with application to spacecraft and space-based networks. *Reliability Engineering and System Safety*. Vol. 99. pp: 123-138.

Castet, J-F. and Saleh, J. H. (2013). Interdependent Multi-Layer Networks: Modeling and Survivability Analysis with Applications to Space-Based Networks. *PLoS ONE*. Vol. 8(4).

CBS. (2014). Road to nowhere: Minor snowstorm brings Atlanta to standstill. *CBS* (29 January). URL: http://www.cbsnews.com/news/atlanta-other-parts-of-south-paralyzed-by-ice-snowstorm/. Accessed 01 October 2014.

Chalupnik, M. J., Wynn, D. D., and Clarkson, J. (2013). Comparison of ilities for protection against uncertainty in system design. Journal of Engineering Design. Vol. 24(12). pp: 814-829.

Chang, S. E., McDaniels, E., Fox, J., Dhariwal, R., and Longstaff, H. (2013). Toward Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgments. *Risk Analysis*. Vol. 34(3). pp 416-434.

Chittister, C. G., and Haimes, Y. Y. (2011). The Role of Modeling in the Resilience of Cyberinfrastructure Systems and Preparedness for Cyber Intrusions. *Journal of Homeland Security and Emergency Management*. Vol. 8 (1).

Clemen, R. T. and Winkler R. L. (1999). Combining Probability Distributions From Experts in Risk Analysis. Risk Analysis. Vol. 19(2). pp: 187-203.

Cox, L.A. (2012). Confronting deep uncertainties in risk analysis. *Risk Analysis*.Vol. 32(10). pp: 1607-1629.

Crossley, W.A. (2004). System of Systems: An Introduction of Purdue University Schools of Engineering's Signature Area. *Engineering Systems Symposium at MIT*. Cambridge, MA. March 29-31.

Crucitti, P., Latora, V., and Marchioori, M. (2004). Model for Cascading Failures in Complex Networks. *Physical Review E*. Vol. 69(4).

Dahmann, J. and Baldwin, K. (2008). Understanding the Current State of US Defense Systems of Systems and the Implications for Systems Engineering. *IEEE Systems Conference*. Montreal, Canada. April 7-10.

Dedman, B. (2011). What are the odds? US nuke plants ranked by quake risk. *NBC News*. URL: http://www.nbcnews.com/id/42103936/ns/world_news-asia_pacific/t/what-are-odds-us-nuke-plants-ranked-quake-risk/#.UznaFq1dUvd. Accessed March 04, 2014.

DeLaurentis, D., Crossley, W., and Mane, M. (2011). Taxonomy to Guide Systems-of-Systems Decision-Making in Air Transportation Problems. *Journal of Aircraft*. Vol. 48(3). pp: 760-770.

DoD. (2008). Systems Engineering Guide for Systems of Systems. Version 1.0. URL: http://www.acq.osd.mil/se/docs/SE-Guide-for-SoS.pdf. Accessed 18 January 2015.

DoD. (2010). The DoDAF Architecture Framework Version 2.02. URL: http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf. Accessed 21 January 2015.

DoD. (2011). Department of Defense Science and Technology Emphasis Areas. URL: http://www.acq.osd.mil/chieftechnologist/publications/docs/OSD%2002073-11.pdf. Accessed 22 January 2015.

Dove, R. (2001). *Response Ability—The Language, Structure, and Culture of the Agile Enterprise*. Wiley. New York.

Dunjo, J., Fthenakis, V., Vilchez, J. A., and Arnaldos, J. (2010). Hazard and operability (HAZOP) analysis. A literature Review. *Journal of Hazardous Materials*. Vol. 19(32). pp: 19-32.

Elsayed, E. (1996). *Reliability Engineering*. Addison Wesley Longman Inc.

Feynman, R. (1986). Personal observations on Reliability of Shuttle. In *NASA Rogers Commission Report - Appendix F*. URL: http://history.nasa.gov/rogersrep/v2appf.htm. Accessed March 03, 2014.

Filippini, R. and Silva, A. (2013). A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies. *Reliability Engineering and System Safety*. Vol. 125. pp: 82-91.

Filippini, R. and Silva, A. (2015). I®ML: An Infrastructure Resilience-Oriented Modeling Language. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. Vol. 45 (1). pp: 157-169.

Fleming, C. H., Spencer, M. Thomas, J., Leveson, N., Wilkinson, C. (2013). Safety assurance in NextGen and complex transportation systems. *Safety Science*. Vol. 55. pp: 173-187.

Folke, C. (2006). Resilience: The emergence of a perspective for social–ecological systems analyses. *Global Environmental Change*. Vol. 16(3). pp: 253-267.

Francis, R. and Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering and System Safety*. Vol. 121. pp: 90-103.

GAO. (2014). Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts. *Government Accountability Office*. URL: http://www.gao.gov/assets/670/665788.pdf. Accessed March 17, 2015.

Garmezy, N. (1970). Process and reactive schizophrenia: Some conceptions and issues. *Schizophrenia Bulletin*. Vol. 1(2). pp: 30–74.

Garvey, P. R. and Pinto, C. A. (2009). Introduction to Functional Dependency Network Analysis. *International Symposium on Engineering Systems*. Cambridge, MA. June 15-17.

Giuliano, G., and Golob, J. (1998). Impacts of the Northridge Earthquake on Transit and Highway Use. *Journal of Transportation and Statistics*. Vol. 1(2). pp: 1-20.

Goerger, S., Madni., A. M., and Eslinger, O. J. (2014). Engineered Resilient Systems: A DoD Perspective. *Conference on Systems Engineering Research*. Redondo Beach, CA. March 21-22.

Goldman, H.; McQuaid, R.; Picciotto, J. (2011). Cyber resilience for mission assurance. *IEEE International Conference on Technologies for Homeland Security*. Waltham, MA. November 15-17.

Goodyear, M., Goerdel, H. T., Portillo, S., & Williams, L. (2010). Cybersecurity management in the states: The emerging role of chief information security officers. *IBM Center for The Business of Government*. Washington, D.C.

Gorod and Sauser. (2008). System-of-Systems Engineering Management: A Review of Modern History and a Path Forward. *IEEE Systems Journal*. Vol. 2(4). pp: 484-499.

Guarniello, G. and DeLaurentis, D. (2013). Dependency Analysis of System-of-Systems Operational and Development Networks. *Conference on Systems Engineering Research*. Atlanta, GA, March 20-22.

Haimes, Y. Y. (2009). On the definition of resilience in Systems. *Risk Analysis*. Vol. 29 (4). pp 498-501.

Haimes, Y.Y. (2012). Strategic preparedness for recovery from catastrophic risks to communities and infrastructure systems of systems. *Risk Analysis*. Vol. 32(11). pp 1834-1845.

Haimes, Y. Y., Crowther, K., and Horowitz, B. M. (2008). Homeland security preparedness: Balancing protection with resilience in emergent systems. *Systems Engineering*. Vol. 11(4), pp 287-308.

Hamel, G., & Valikangas, L. (2003).The quest for resilience. *Harvard Business Review.* Vol. 81. pp: 52–63.

Han, S.Y., Marais, K., and DeLaurentis, D. (2012). Evaluating System of Systems Resilience using Interdependency Analysis. *IEEE International Conference on Systems, Man, and Cybernetics, Seoul, Korea*. October 14-17.

Henry, D. and Ramirez-Marquez, H. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering and System Safety*. Vol. 99. pp: 114-122.

Higgins, A. (2012). Lessons for the U.S. From a Flood-Prone Land. *New York Times* (14 November). URL: http://www.nytimes.com/2012/11/15/world/europe/netherlands-sets-modelof-flood-prevention.html?pagewanted=all. Accessed 01 October 2014.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, Vol. 4, pp: 1–23.

Holling, C. S. (1996). Engineering resilience versus ecological resilience. In Schulze, P. ed. *Engineering within Ecological Constraints*. The National Academies Press. Washington, D.C.

Hollnagel, E. (2012). *FRAM, the functional resonance analysis method modelling complexsociotechnical systems*. Ashgate. Surrey, England

Hollnagel, E., Woods, D. W., and Leveson, N. (2006). *Resilience Engineering: Concepts and Precepts*. Ashgate. Burlington, VT.

INCOSE. (2000), Resilient Systems Working Group. URL: http://www.incose.org/practice/techactivities/wg/rswg/. Accessed 22 January 2015.

Jackson, S. (2007). A multidisciplinary framework for resilience to disasters and disruptions. *Journal of Integrated Design and Process Science*. Vol. 11(2). pp: 91-108. Jackson and Ferris. (2013). Resilience Principles for Engineered Systems. *Systems Engineering*. Vol. 16(2). pp: 152-164.

Jackson, S. (2010). *Accident Avoidance and Survival and Recovery from Disruptions*. Wiley. Hoboken, NJ

Jackson, S. and Ferris, T. L. J. (2013). Resilience Principles for Engineered Systems. *Systems Engineering*. Vol. 16(2). pp: 152-164

Jamshidi, M. (2008). System of systems engineering - New challenges for the 21st century. *IEEE Aerospace and Electronic Systems Magazine*. Vol. 23(5). pp: 4-19.

Johansson, J., and Hassel, H. (2010). An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering and System Safety*. Vol. 95(12), pp: 1335–1344.

Johansson, J., Hassel, H., and Zio, E. (2013). Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. *Reliability Engineering and System Safety*. Vol. 120, pp: 27–38.

Johnson, J. L. and Wielchelt, S. A. (2004). Introduction to the special issue on resilience. *Substance Use and Misuse*. Vol. 39(5). pp: 657–670.

Kalawsky, R.S., Joannou, Y. T., and Fayoumi, A. (2013). Using architecture patterns to architect and analyze systems of systems. *Conference on Systems Engineering Research*. Atlanta, GA. 20-22 March.

Kantur, D. and Iseri-Say, A. (2012). Organizational resilience: A conceptual integrative framework. *Journal of Management & Organization*. Vol. 18(6), pp: 762–773.
Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, Vol. 1. pp: 11–28.

Kaplan, S. and Garrick, B. J. (1981). On the quantitative definition of risk. Risk Analysis, Vol. 1.pp: 11–28.

Kaufman, S., Qing, C., Levenson, N., and Hanson, M. (2012). Transportation During and After Hurricane Sandy. URL: http://wagner.nyu.edu/files/rudincenter/sandytransportation.pdf. Accessed March 03, 2015.

Klein, R. J. T., Smit, M. J., Goosen, H., and Hulsbergen, C. H. (1998). Resilience and vulnerability: coastal dynamics or Dutch dikes. *Geographical Journal*. Vol. 164(3). pp: 259–268.

Klein, R. J. T, Nicholls, R. J., and Thomalla, F. (2003). Resilience to natural hazards: How useful is this concept?. *Environmental Hazards*. Vol. 5. pp: 35–45.

Knight, J.C. (2002). Safety critical systems: challenges and directions. *Proceedings of the 24th International Conference on Software Engineering*. Orlando, FL. 25-25 May.

Koutsopoulos, H. N. and Wang, Z.(007). Simulation of Urban Rail Operations: Application Framework, *Transportation Research Record: Journal of the Transportation Research Board*. pp: 84-91.

Kurant, M. and Thiran, P. (2007). Error and Attack Tolerance of Layered Complex Networks. *Physical Review E.* Vol. 76(2).

Laprie, J-C. (2008). From dependability to resilience. *IEEE International Conference on Dependable Systems and Networks*. pp: G8–G9.

Lengnick-Hall, C. A. and Beck, T. E. (2003). Beyond bouncing back: The concept of organizational resilience. Paper presented at the National Academy of Management meetings. Seattle, WA.

Leveson, N. (1995). *Safeware*. Addison-Wesely. Boston, MA.

Leveson, N. (2012). *Engineering a Safer World*. The MIT Press. Cambridge, MA.

Liu, Y-Y., Slotine, J-J., and Barabasi, A-L. (2011). Controllability of complex networks. *Nature*. Vol. 473(12). pp: 167–173.

Lopez, D. (2006). Lessons Learned From the Front Lines of the Aerospace. *IEEE International Conference on System of Systems Engineering*. Los Angeles, CA.

Luzeaux, D. (2011). Engineering Large-scale complex systems. In Luzeaux, D., Ruault, J-R., and Wippler, J-L., eds. *Complex Systems and Systems-of-Systems Engineering*. Wiley. Somerset, NJ.

Mahnken, G. E. (2001). Use case histories to energize your HAZOP. *Chemical Engineering Progress*. Vol. 97(3). pp: 73-78.

Masten, A. S. (1994). Resilience in individual development. Successful adaptation despite risk and adversity. In Wang, M. C., Gordon, E. W., eds. *Educational Resilience in Inner-City America: Challenges and Prospects*. Erlbaum. Hillsdale, NJ. pp: 3–25.

Madni, A. M. (2010). Integrating humans with software and systems: Technical challenges and a research agenda. *Systems Engineering*. Vol. 13 (3). pp: 232-245.

Madni., A. M., and Jackson, S. (2009). Towards a Conceptual Framework for Resilience Engineering. *IEEE Systems Journal*. Vol. 3(2). pp: 181-191.

Maier, M. W. (1998). Architecting Principles for System-of-systems. *Journal of Systems Engineering*. Vol. 1(4). pp: 267-284.

Maier, M. W. and Rechtin, E. (2000). *The Art of Systems Architecting*. CRC Press - Boca Raton, FL.

Mallak, L. A. (1998). Measuring resilience in health care provider organizations. *Health Manpower Management.* Vol. 24(4). pp: 148–152.

Mane, M., Crossley, W. A., and Nusawardhana. (2007). System of Systems Inspired Aircraft Sizing and Airline Resource Allocation via Decomposition. *Journal of Aircraft*. Vol. 44(4). pp: 1222-1235.

Manyena, S. B. (2006). The concept of resilience revisited. *Disasters.* Vol. 30(4). pp: 434–450.

Marais, K. and Weigel, A. (2006). A Framework to Encourage Successful Technology Transition in Civil Aviation. *25th Digital Avionics Systems Conference*. Portland, OR. 15-19 October.

MBTA. (2014a). Massachusetts Bay Transportation Authority: Rapid Transit/Key Bus Routes Map. URL: http://www.mbta.com/uploadedfiles/Documents/Schedules_and_Maps/Rapid%20Transit%20w%20Key%20Bus.pdf. Accessed March 01, 2015.

MBTA. (2014b). Massachusetts Bay Transportation Authority: Ridership and Service Statistics. URL: http://www.mbta.com/uploadedfiles/documents/2014%20BLUEBOOK%2014th%20Edition.pdf Accessed March 01, 2015.

McCarter, B. G. and White, B. E. (2007). Emergence of SoS, Socio-Cognitive Aspects. In Jamshidi, M. ed. *System of Systems Engineering- Principles and Applications*. CRC Press.

Mekdeci, B., Ross, A. M., Rhodes, D. H., and Hastings, D. E. (2012). Controlling Change within Complex Systems Through Pliability. *Third International Engineering Systems Symposium (CESUN)*. Delft, Holland. June 18-20.

Miles, S. B. and Chang, S. E. (2006). Modeling community recovery from earthquakes. *Earthquake Spectra*. Vol. 22(2). pp: 439‑458.

Modarres, M., Kaminsky, M., and Krivtsov, V. (1999). *Reliability Engineering and Risk Analysis: A Practice Guide*. Marcel Dekker. New York, NY.

Motter, A.E. and Lai, Y-C. (2002). Cascade-Based Attacks on Complex Networks. *Physical Review E*. Vol. 66(6).

Neches, R. and Madni, A. M. (2012). Towards affordably adaptable and effective systems. *Systems Engineering.* Vol. 16(2). pp: 224-234.

Newman, D. E., Nkei, B., Carreras, B. A., Dobson, I., Lynch, V. E., et al. (2005). Risk Assessment in Complex Interacting Infrastructure Systems. *38th Hawaii International Conference on System Sciences*. Big Island, HI. January 03-06.

NIPP: (2006). National Infrastructure Protection Plan. *Department of Homeland Security.* URL: http://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf. Accessed July 20, 2014.

NYC. (2013). Hurricane Sandy after Action: Report and Recommendations to Mayor Michael R. Bloomberg. URL:http://www.nyc.gov/html/recovery/downloads/pdf/sandy_aar_5.2.13.pdf. Accessed March 26, 2015.

Okashah, L.A. and Goldwater, P.M. (1994). Unknown unknowns: modeling unanticipated events. In Tew, J. D., Manivannan, M. S., Sadowski, D. A., and Seila, A. F., eds. *Proceedings of the 1994 Winter Simulation Conference.* pp: 689-694.

Open Group. (2011). The Open Group Architectural Framework Version 9.1. URL: http://www.opengroup.org/togaf/. Accessed 21 January 2015.

Ouyang, M., Dueñas-Osorio, L., and Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Structural Safety*. Vol. 36 (1). pp: 23–31.

Paltrinieri, N., Tugnoli, A., Bonvicini, S., Cozzani, V. (2011). Atypical scenarios identification by the DyPASI procedure: application to LNG. *Chemical Engineering Transactions.* Vol. 24. pp: 1171-1176.

Pant, R., Barker, K., and Zobel, C.W. (2013). Static and Dynamic Metrics of Economic Resilience for Interdependent Infrastructure and Industry Sectors. *Reliability Engineering and System Safety*. Vol. 125. pp: 92-102.

Park, J., Seager, T. P., Rao, P. S. C., Convertino, M., and Linkov, I.. (2013). Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. *Risk Analysis*. Vol. 33(3). pp: 356-367.

Pearson, I. L. G. (2011). Smart grid cyber security for Europe. *Energy Policy*. Vol. 39(9). pp: 5211-5218.

Pender, B., Currie, G., Delbosc, A., and Shiwakoti, N. (2013). Disruption recovery in passenger railways. *Transportation Research Record: Journal of the Transportation Research Board* . Vol. 2353(4). pp: 22-32.

PPD. (2013). Presidential Policy Directive: Critical Infrastructure Security and Resilience. URL: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Accessed January 26, 2015.

Provan, K. G. and Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*. Vol. 18(2). pp: 229-252.

Ramirez-Marquez, J.E. and Coit, D. W. (2007). Multi-state component criticality analysis for reliability improvement in multi-state systems. *Reliability Engineering & System Safety.* Vol. 92(12). pp: 1608-1619.

Rasmussen, N. (1975*). Reactor Safety Study (WASH-1400)*, US Nuclear Regulatory Commission, NUREG-75/014.

Rausand, M., and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley – Interscience. Hoboken, NJ.

Reed, D. A., Kapur, K. C., and Christie, R. D. (2009). Methodology for assessing the resilience of networked infrastructure. *IEEE Systems Journal*. Vol. 3(2). pp: 174–180.

Renschler, C. S., Frazier, A. E., Arendt, L. A. Cimellaro, G. P., Reinhorn, A. M., and Bruneau, M. (2010). Developing the 'PEOPLES' resilience framework for defining and measuring disaster resilience at the community scale. *9th US and 10th Canadian Conference on Earthquake Engineering.* Toronto, Canada, July 25-29, 2010.

Resilience Alliance. (2001). URL: http://www.resalliance.org/. Accessed 22 January 2015.

Richards, M.G. (2009). Multi-attribute tradespace exploration for survivability. PhD Dissertation. Massachusetts Institute of Technology.

Richards, M. G., Ross, A. M, Shah, N. B., and Hastings, D. E. (2009). Metrics for Evaluating Survivability in Dynamic Multi-Attribute Tradespace Exploration. *Journal of Spacecraft and Rockets*. Vol. 46(5).

Righi, A. W., Saurin, T. A., and Wachs, P. (2015). A systematic literature review of resilience engineering: Research areas and a research agenda proposal. *Reliability Engineering & System Safety*. doi:10.1016/j.ress.2015.03.007.

Rinaldi, S.M. (2004). Modeling and Simulating Critical Infrastructures and Their Interdependencies. *37th Hawaii International Conference on System Sciences*. Big Island, HI. January 05-08.

Rinaldi, S.M., Peerenboom, J. P., and Kelly, T.K. (2001). Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*. Vol. 21(6). pp: 11-25.

Robinson, B. W. (1995). Application of hazard and operability studies to a wide range of industries and activities. *Quality and Reliability Engineering International*. Vol. 11(6). pp:. 399–402.

Rose, A. (2007). Economic resilience to natural and man-made disasters: multi-disciplinary origins and contextual dimensions. *Environmental Hazards*. Vol. 7(4). pp: 383-398.

Rouse, W. (2012). Multi-Level Socio-Technical Modeling. *Systems Engineering Research Center Project #44* . URL: http://www.sercuarc.org/projects/view/34. Accessed April 03, 2014.

Ruault, J-R., Vanderhaegen, F., and Luzeaux, D. (2012). Sociotechnical systems resilience. *INCOSE International Symposium*. Vol. 22(1). pp:339-354.

Ryan, E. T., Jacques, D. R., and Colombi, J. M. (2013). An Ontological Framework for Clarifying Flexibiliy-Related Terminology via Literature Survey. *Systems Engineering*. Vol. 16(1). pp: 99-109.

Saleh, J. H., Mark, G., and Jordan, N. C. (2009). Flexibility: a multi-disciplinary literature review and a research agenda for designing flexible engineering systems. *Journal of Engineering Design*. Vol. 20(3). pp: 307-323.

Saleh, J. H., Marais, K. B., and Favaró, F. M. (2014). System safety principles: A multidisciplinary engineering perspective. *Journal of Loss Prevention in the Process Industries*. Vol. 29. pp: 283-294.

SEI. (2009). Software Engineering Institute – CERT Resiliency Engineering Framework.

Sheard, S. and Mostashari, A. (2008). A Framework for System Resilience Discussions. *18th Annual International Symposium of INCOSE*. Utrecht, Netherlands. 15-19 June.

Sheffi, Y. (2007). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. The MIT Press. Cambridge, MA.

Sheffi, Y. and Rice, J. B. (2005). A supply chain view of the resilient enterprise. MIT Sloan Management Review. Vol. 47(1).

Shinozuka, M., Chang, S. E., Cheng, T-C., Feng, M., O'Rourke, T. D., Saadeghvaziri, M. A., Dong, X., Jin, X., Wang, Y. and Shi, P. (2004). Resilience of Integrated Power and Water Systems. In *MCEER Research Progress and Accomplishments: 2003-2004* ed. MCEER). Buffalo, NY.), pp: 65-86.

Sterbenz, J. P. G., Cetinkaya, E. K., Hameed, M. A., Jabbar, A., and Rohrer, J. P. (2011). Modelling and Analysis of Network Resilience. *International Conference on Communication Systems and Networks (COMSNETS)*. Bangalore, India. January.

Storey, N. R. (1996). *Safety Critical Computer Systems*. Addison-Wesley. Boston, MA.

SYSTRA. (2014). RAILSIM X. URL: http://www.systraconsulting.com/railsim-xreg.html. Accessed March 12, 2015.

Thissen, W. A. H., and Herder, P. M. (2008). System of System Perspectives on Infrastructures. In Jamshidi, M. ed. *System of Systems Engineering- Principles and Applications*. CRC Press.

Tierney, K. (2003). Conceptualizing and measuring organizational and community resilience: Lessons from the emergency response following the September 11, 2001 attack on the World Trade Center. *Third Comparative Workshop on Urban Earthquake Disaster Management*. Kobe, Japan.

Tierney, K. and Bruneau, M. (2007). Conceptualizing and Measuring Resilience. *TR News.* URL: http://onlinepubs.trb.org/onlinepubs/trnews/trnews250_p14-17.pdf. Accessed March 01, 2014.

Trucco, P., Cagno, E., and Ambroggi, M. D., (2012). Dynamic functional modeling of vulnerability and interoperability of Critical Infrastructures. *Reliability Engineering and System Safety*. Vol. 105. pp: 51-63.

TTCP. (2014). Recommended Practices: System of Systems Considerations in the Engineering of Systems. The Technical Cooperation Program (TTCP) Technical Report. URL: http://www.acq.osd.mil/se/docs/TTCP-Final-Report-SoS-Recommended-Practices.pdf. Accessed 18 January 2015.

Uday, P., and Marais, K. (2013). Exploiting Stand-In Redundancy to Improve Resilience in a System-of-Systems (SoS). *Conference on Systems Engineering Research.* Atlanta, GA. March 20-22.

Ulieru, M. (2007). Design for resilience of networked critical infrastructures. *IEEE International Conference on Digital Ecosystems and Technologies*. Cairns, Australia. February 21-23.

Vaidhyanathan, R. and Venkatasubramianian, V. (1995). Digraph-based models for automated HAZOP analysis. *Reliability Engineering and System Safety*. Vol. 33(49). pp:. 33-49.

Van der Borst, M., and Schoonakker, H. (2001). An overview of PSA importance measures. *Reliability Engineering & System Safety*. Vol. 72 (3). pp: 241-245.

Van der Leeuw, S.E. and C.A. Leygonie. (2000). A long-term perspective on resilience in socio-natural systems. *Workshop on System Shocks–System Resilience*. Abisko, Sweden. May 22-26.

Weber, P. and Jouffe, L. (2006). Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN). *Reliability Engineering and System Safety*. Vol. 91(2). pp: 149-162.

WEC. (2013). Building Resilience in Supply Chains. World Economic Forum. URL: http://www.weforum.org/reports/building-resilience-supply-chains. Accessed 01 October 2014.

Weick, K. E., Sutcliffe K. M., and Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. *Research in Organizational Behavior.* Vol. 21. pp: 81–123.

Werner, E. E. and Smith, R. S. (1977). *Kauai's children come of age*. University of Hawaii Press. Honolulu, HI.

White, B.E. (2006). Fostering Intra-Organizational Communication of Enterprise Systems Engineering Practices. *National Defense Industrial Association (NDIA) 9th Annual Systems Engineering Conference*. San Diego, CA. October 23-26.

Whitson, J. C., and Remirez-Marquez, J. E. (2009). Resiliency as a component importance measure in network reliability. *Reliability Engineering and System Safety*. Vol. 94(10). pp: 1685-1693.

Wildavsky, A. (1991). *Searching for safety*. Transaction Publishers. New Brunswick, NJ.

Wojcik, L.A. and Hoffman, K.C. (2006). Systems of Systems Engineering in the Enterprise Context: A Unifying Framework for Dynamics. *IEEE International Conference on System of Systems Engineering*. Los Angeles, CA.

Wreathall, J. (2006). Property of Resilient Organization: An Initial View. In Hollnagel, E., Woods, D. W., and Leveson, N. eds. *Resilience Engineering: Concepts and Precepts*. Ashgate. Burlington, VT.

Xu, X-L., Qu, Y-Q., Guan, S., Jiang, Y-M., and He, D-R. (2011). Interconnecting Bilayer Networks. *Europhysics Letters*. Vol. 93.

Yue, O.C. (2003). Cyber security. *Technology in Society*. Vol. 25(4). pp: 565-569.
Zhang, W. J., and Lin, Y. (2010). On the principle of design of resilient systems – application to enterprise information systems. *Enterprise Information Systems*. Vol. 4(2). pp: 99-110.

Zhang, W. J., and Lin, Y. (2010). On the principle of design of resilient systems – application to enterprise information systems. *Enterprise Information Systems*. Vol. 4(2). pp:. 99-110.

Zio, E., and Ferrario, E. (2013). A framework for the system-of-systems analysis of the risk for a safety-critical plant exposed to external events. *Reliability Engineering & System Safety*. Vol. 114. pp: 114-125.

Zobel, C. W. (2011). Representing perceived tradeoffs in defining disaster resilience. *Decision Support Systems*. Vol. 50(2). pp: 394-403

VITA

VITA

Payuna Uday completed her schooling in Dubai and holds a Bachelor of Technology in Electronics and Communication Engineering from the National Institute of Technology in Trichy, India.

In 2011 Payuna received her master's degree in Aeronautics and Astronautics from Purdue University, with a focus on assessing the environmental mitigation potential of operational changes in aviation.

Working in the VRSS (Value through Reliability, Safety, and Sustainability) Lab under the guidance of Prof. Karen Marais, she has gained experience in systems engineering and risk assessment of complex socio-technical systems in general and, air transportation systems in particular.